Deloitte.

Informationssäkerhet

Skara kommun

Juni 2022

Innehåll

Sammanfattning

Deloitte AB har av de förtroendevalda revisorerna i Skara kommun fått uppdraget att genomföra en granskning avseende informationssäkerhet och kommunens beredskap att upprätthålla denna i händelse av en krasch eller längre avbrott.

Revisionsfråga

Har Skara kommun/kommunstyrelsen en tillräckligt god beredskap för att kunna upprätthålla en god informationssäkerhet och en god verksamhet även i händelse av en IT-krasch eller längre IT-avbrott?

Svar på revisionsfråga

Vår sammanfattande bedömning är att Skara kommun/kommunstyrelsen i dagsläget endast delvis har en god beredskap för att upprätthålla en god informationssäkerhet och en god verksamhet i händelse av en IT-krasch eller längre IT-avbrott.

Iakttagelser

- De policies och riktlinjer som finns för informationssäkerhet är av äldre modell och utgår främst från BITS vilket är en äldre standard. En enklare informationsklassning pågår.
- Frågorna har innan 2021/22 inte fått kommunstyrelsens uppmärksamhet. De brister som observerades vid en genomgång av informationssäkerheten 2017 har ännu inte åtgärdats fullt ut. Informationssäkerheten har under 2022 fått mer uppmärksamhet än tidigare på kommunledningsnivå. Kommunen har därför beslutat anställa en informationssäkerhetssamordnare fr om augusti 2022. Kommunstyrelsen bör fortsatt stärka sin insyn och uppsikt över kommunens informationssäkerhet.
- Frågorna kring informationssäkerhet har främst ansetts röra IT-säkerhet vilket dock bara är en delmängd. För en god informationssäkerhet finns många aspekter att ta hänsyn till och hela organisationen behöver spela sina roller för att få ihop helheten på bästa sätt.
- Kommunens IT-leverantör är kommunalförbundet Göliska IT. Ansvarsförhållandena mellan kommunen och Göliska upplevs i praktiken som otydliga. I och med att Göliska inrättades försvann IT-kompetens från kommunen vilket upplevs ha försvårat arbetet med informationssäkerhet och kravställning mot Göliska IT.
- Inom samverkansorganisationerna V6 och SMS pågår också aktiviteter som påverkar Skara kommuns informationssäkerhet. Även detta arbete bör integreras i Skara kommuns arbete för att stärka informationssäkerheten. I dagsläget är det svårt att få en överblick över hur alla delar hänger ihop och hur dessa påverkar helheten för informationssäkerheten. Utöver Göliska, V6 och SMS samarbetar Skara kommun även med Lidköping vad gäller upphandling. Att samordna alla aktiviteter och aktörer kräver god samordning, tydliga ansvarsförhållanden och god uppföljning. Annars riskerar det att uppstå luckor vilka kan påverka kommunens beredskap och faktiska informationssäkerhet.
- De effekter som en IT-krasch eller längre IT-avbrott skulle kunna få på verksamheten är inte kartlagda. Dvs. kommunen har pga den låga uppmärksamhet som området haft inte gjort en risk eller gapanalys för att kartlägga IT-beroenden. Även samband mellan system och vilka rutiner som finns i kommunen för att hantera ett längre avbrott behöver kartläggas. Det pågår vissa insatser för att genomföra en sådan analys för delar av organisationen.

.

Rekommendationer

Vi rekommenderar kommunstyrelsen att;

- Slutföra arbetet med nya policies och riktlinjer för informationssäkerhet.
- Tydliggöra ansvarsförhållanden gentemot IT-leverantören Göliska samt övriga samarbetspartners så att det finns en sammanhållen bild över de förhållanden och aktörer som påverkar informationssäkerheten i Skara kommun. Arbetet med att få god informationssäkerhet behöver präglas av god samordning, tydliga ansvarsförhållanden och god uppföljning.
- Skapa en helhetsbild av ansvarsförhållanden och arbetsuppgifter rörande informationssäkerhet i syfte att undvika luckor i arbetet och åtgärder.
- Säkerställa att det finns en heltäckande och uppdaterad kontinuitetsplanering för IT-verksamheten som täcker de områden Skara kommun anser mest väsentliga. Tex. vilka system bör återstartas först.
- Att genomföra riskanalys och gapanalys för hela verksamheten i syfte att klarlägga vilka risker som kommunen/kommunstyrelsen bör agera på. Detta i syfte att se till att informationen är tillgänglig, riktig och skyddas mot obehörig insyn.
- Genomföra en analys av vilka effekter och konsekvenser ett längre IT-avbrott skulle medföra för kommunens verksamhet och vilka alternativa arbetssätt som kan tillämpas för de viktigaste uppgifterna.
- Att genomföra en klassning av all information i syfte att säkerställa att kommunens information har en lämplig nivå av skydd. Känslig information behöver ett högre skydd än information som är mindre känslig.
- Införa en strukturerad uppföljning för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad och har den avsedd verkan. Uppföljningen bör också fokusera på om valda säkerhetsåtgärder fungerar tillfredsställande och ger de effekter som tänkt. Kommunen/kommunstyrelsen kan genom detta se att informationssäkerhetsarbetet med tillhörande riskhantering har avsedd funktion och verkan. Beslut om ändringar i åtgärder bör fattas löpande utifrån analys av hotbild.
- Överväg att införa en funktion för tjänsteman i beredskap (TIB) i syfte att tydliggöra och stärka kommunikationen vid kriser och ev. incidenter.
- Genomföra nödvändiga utbildningar inom organisationen.

Jönköping den 30 juni 2022

DELOITTE AB

Annika C Karlsson
Projektledare

Shkurte Bilalli
Projektmedarbetare

1. Inledning

Bakgrund

Skara kommun är som alla kommuner starkt beroende av en fungerade IT-miljö och att kommunen och dess anställda har åtkomst till uppgifter i digitalt format. Detta brukar sammanfattas i begreppet informationssäkerhet. Alla kommuner löper risk att tillgången till uppgifter och information bryts pga IT-haveri av något slag eller att intrång sker som gör att systemen blir obrukbara över en längre tid. För att motverka att en sådan händelse får allvarliga konsekvenser för kommunen bör det finnas en planering för hur sådana incidenter ska hanteras. IT används i de flesta processer och informationen behöver vara tillgänglig, korrekt och åtkomlig i princip 24/7 alla årets dagar.

Kommunen bör ha en god planering i form av informationssäkerhetspolicy, kontinuitetsplanering och alternativa arbetssätt m.m. Detta för att i möjligaste mån undvika vissa incidenter men även för att kunna hantera incidenter den dag de ev inträffar. Då IT-tjänsterna är outsourcade krävs också att Skara kommun ställt tillräckliga krav på leverantören Göliska IT tex i form av servicenivåöverenskommelse, återstartsplaner, krav på back-up och redundans etc. Ansvaret för informationssäkerheten kan inte outsourcas utan vilar fortsatt på kommunen.

Revisorerna önskar få en kartläggning av hur Skara kommun planerar och agerar för att hålla en god informationssäkerhet. Detta inkluderar att kommunen har nödvändiga policies och planer på plats samt att kommunen agerar i enlighet med dessa. En god informationssäkerhet kräver också en plan för hur incidenter ska kunna hanteras – dvs. hur kommunens verksamhet kan fortgå med så liten störning som möjligt vid en större incident. Finns manuella rutiner, alternativa arbetssätt på plats? Samt kommer kommunens information i ekonomi och verksamhetssystem att vara åtkomlig och oförvanskad efter en ev incident. Detta kräver att en kontinuitets- och katastrofplanering finns på plats så att kommunen så snabbt som möjligt kan återgå till en normal verksamhet. I granskningen ingår också en kartläggning av vilka krav som kommunen ställt på underleverantören Göliska IT. Vi kartlägger också vilken återkoppling som kommunstyrelsen får kring informationssäkerhetsläget i Skara kommun.

Med utgångspunkt från ovanstående och revisorernas riskanalys för år 2022 har revisorerna gett Deloitte i uppdrag att presentera ett förslag till en granskning.

Syfte och avgränsning

Granskningens syfte är kartlägga hur Skara kommun/kommunstyrelsen planerar och agerar för att hålla en god informationssäkerhet. Granskningen har begränsats till kommunstyrelsen och de planer och uppföljningar som genomförs inom informationssäkerhetens område.

Revisionsfråga

Har Skara kommun/kommunstyrelsen en tillräckligt god beredskap för att kunna upprätthålla en god informationssäkerhet och en god verksamhet även i händelse av en IT-krasch eller längre IT-avbrott?

Underliggande frågeställningar

- Vilka styrande dokument och planer finns avseende informationssäkerhet?
- Hur agerar kommunen för att upprätthålla en god informationssäkerhet generellt. Vilka åtgärder avser kommunen vidta i händelse av en IT-krasch eller vid ett längre IT-avbrott?
- Har kommunen kartlagt vilka effekter ett avbrott skulle få på den dagliga verksamheten, tex på trygghetslarm?
- Har kommunen ställt tillräckliga krav på sin IT-leverantör?
- Vilken återkoppling lämnas till kommunstyrelsen angående informationssäkerhetens status och vilka åtgärder vidtas?

Metod och granskningsinriktning

Granskningen genomförs genom dokumentgranskning, protokollsgranskning samt intervjuer med utvalda nyckelpersoner med följande befattningshavare:

- Kommunstyrelsens ordförande
- Kommundirektören
- Chefsjurist
- Kommunikationschef
- Säkerhetssamordnare
- Digitaliseringsstrateg

Granskningen har delats in i följande sju faser:

- Planering av intervjuer.
- Samla fakta/underlag genom intervjuer och dokumentgranskning.
- Genomgång, sammanställning och analys av insamlat material. Vid behov komplettering med mer material.
- Framtagning av viktiga iakttagelser och rekommendationer samt svar på revisionsfråga.
- Rapportskrivning inkl. sakavstämning.
- Presentation av granskning till revisorer.
- Godkänd rapport skickas till berörda nämnder & revisorer.

Revisionskriterier

Kommunallagen. En bedömning av kommunens styrande dokument kommer göras mot kriterier i gällande standard på området.

Kvalitetssäkring

Kvalitetssäkring har skett genom Deloittes interna kvalitetssäkringssystem. Rapporten har även kvalitetssäkrats av de intervjuade personerna.

2. Granskningsresultat

Utifrån genomförda intervjuer och granskat material har en övergripande beskrivning av informationssäkerhet gjorts nedan. De iakttagelser som framkommit till följd av intervjuer och dokumentstudier redogörs under den rubrik som ansetts mest lämplig.

Vilka styrande dokument och planer finns avseende informationssäkerhet?

Kommentar och bedömning

Skara kommun har vissa beslutade riktlinjer för informationssäkerhet men dessa är från 2007 och bygger på den äldre BITS-standarden. Dessa riktlinjer är tämligen generella och ger inte en heltäckande planering eller uppföljning. Utöver detta finns kompletterande riktlinjer för informationssäkerhet för omsorgen samt för säkerhetsskyddsfrågor. Samverkansorganet V6 har arbetat fram vägledningsdokument men dessa har Skara kommun inte beslutat om ännu då man anser att de inte är tillräckliga för kommunens ändamål. Kommunens digitaliseringsstrateg har delvis arbetet om dessa för att få dokumentet klara för beslut.

Kommunalförbundet Göliska IT är kommunens leverantör av IT-tjänster. Det finns ett avtal där förbundets och kommunens uppgifter och ansvar regleras. I avtalet kan man läsa att*; förbundet är primär leverantör av IT-tjänster och stöd för kommunernas digitaliseringsarbete. Samverkan, dialog och transparens ska genomsyra det gemensamma utvecklingsarbetet parterna emellan. Förbundet har en skyldighet att påvisa brister och risker inom Förbundskommunernas informationshantering ur ett IT- och informationssäkerhetsperspektiv. Parterna ska gemensamt med resurser från resp organisationer ständigt arbeta med riskeliminering alt riskminimering. Förbundet ska inom sitt LIS-arbete ansvara för och införa de fysiska och tekniska skydd som man anser nödvändigt för att kunna uppfylla sitt uppdrag gentemot förbundskommunerna. För att upprätthålla lagstadgad nivå och önskvärd kvalitet inom informationssäkerhetsarbetet inom och mellan förbundskommunerna och förbundet är det nödvändigt att samtliga parter tillsätter den organisation och de roller/resurser som krävs inom detta område.*

Förbundskommunerna ska inneha resurser och kompetens för att klassa den information man själva äger för att förbundet ska få förutsättningar att tillsätta rätt skyddsnivå för respektive skyddsklass. Förbundskommunerna bör ha ett etablerat ledningssystem för informationssäkerhet LIS. Digitaliseringsstrateg ska delta i styrning av det löpande IT/informationssäkerhetsarbetet inom samarbetet.

I praktiken verkar det inte fungera som tänkt i avtalet. Skara kommun har inte något etablerat ledningssystem för informationssäkerhet (LIS). Ett sådant system bygger på att ansvarsförhållanden, tydliga arbetsuppgifter och aktiviteter planerats, att utbildning och ledningens uppföljning också finns på plats. Flera delar i detta ledningssystem saknas till stor del i dagsläget. Rollerna för kommunen och kommunalförbundet upplevs som otydliga. I samband med inrättandet av Göliska upplevs kompetens ha försvunnit från kommunen vilket gör att kommunen inte haft förutsättningar för att driva ett bra informationssäkerhetsarbete.

Enligt de vi intervjuat har frågorna först under 2021/22 fått uppmärksamhet och ett arbete påbörjats med att förbättra förutsättningarna. De åtgärder som vidtagits beskrivs som reaktiva och ad-hoc. Kommunikationen i förvaltningarna om vem som ska göra vad har inte fungerat utan till stor del har kommunen förlitat sig på Göliska. För flera frågor lyfter kommunen behovet av att ha en god kompetens för att kunna ställa rätt krav på Göliska. Samt för att kunna bedriva ett bra arbete kring informationssäkerhet. Då kommunen har anställt en informationssäkerhetsamordnare samt frågorna fått genomslag i kommunstyrelsen har Skara kommun påbörjat arbetet. Men det kommer ta ett antal år att få ett ledningens informationssystem på plats.

I dagsläget upplevs ansvars- och arbetsfördelningen mellan Göliska och kommunen som otydlig. För att förhindra att frågor och åtgärder faller mellan stolarna och ev orsakar kommunen väsentlig skada bör fördelningen förtydligas.

Då arbete kring informationssäkerhet även pågår inom ramen för samverkan V6 och SMS (Samhällsskydd mellersta Skaraborg) är det viktigt att allt arbete koordineras med och mellan samtliga parter. Samarbetena kan ge Skara kommun värdefulla verktyg men behöver samordnas bättre så att de verkar mot samma mål och inte på något sätt motverkar varandra. I dagsläget är det oklart hur dessa samarbeten påverkar informationssäkerhetens status och hur alla samarbeten påverkar helheten. Dvs. drar alla samarbeten åt samma håll i samma fråga?

Noterbart också att det i dagsläget inte finns någon informationsklassning av all den information som kommunen har. Det har gjorts ansatser till att använda en förenklad metod för att genomföra detta. Kommunen överväger att införa en TIB-funktion (tjänsteman i beredskap) inom kommunen för att stärka beredskapen.

Nämnas kan också att det 2017 gjordes en kartläggning av informations-säkerhetsnivån i Skara kommun. Av de 18 punkter kartläggningen omfattade nådde endast 3 en acceptabel nivå enligt utredaren. Bl.a. pekades på brister i rapportvägar vid incidenter. Det pekades också på brister i kontinuiteten kring informationssäkerhet. Genomgången omfattade analys av informationssäkerhetsrisker, informationsklassning, ledning/styrning och kontroll, utbildning, säkerhetsåtgärder, uppföljning/utvärdering och upphandling, säkerhetskultur etc. Den maximala poängsumman för delarna varierade mellan 16 till 47 poäng. Den poängsumma Skara bedömdes ha för respektive fråga varierade mellan 0 och 5 vid genomgången 2017.

Bland de åtgärder kommunen sedan dess infört är nytt system för behörighets-tilldelning samt en ny modul för hantering av lösenord. Kommunen bör uppdatera denna genomgång för att få en dagsaktuell bild av läget samt fatta beslut om vilka åtgärder som bör genomföras. Samt besluta om en tidsplan för åtgärder som anses kritiska för informationssäkerheten.

Kommunen/kommunstyrelsen bör upprätta och besluta om nödvändiga dokument på området.

Hur agerar kommunen för att upprätthålla en god informationssäkerhet generellt. Vilka åtgärder avser kommunen vidta i händelse av en IT-krasch eller vid ett längre IT-avbrott?

Kommentar och bedömning

Kommunen har idag inget etablerat LIS-system samt upplever sig inte heller i dagsläget ha tillräcklig kompetens eller resurser för att upprätthålla ett sådant

system. Kommunen beskrivs som känslig pga att grundarbetet inte gjorts. Det har varit mycket fokus på IT-säkerhet och Göliska men informationssäkerhet är ett mycket vidare område än IT-säkerhet. Då kompetensen inte finns kvar inom kommunen upplevs det som svårt göra beställningar till Göliska kring system etc. Om ett längre IT-avbrott skulle inträffa behövs en beredskap för att tillämpa alternativa eller manuella rutiner.

I dagsläget upplever de intervjuade att det är oklart vem som bör kontaktas vid en IT-krasch m.m. då kommunen ännu inte har en tjänsteman i beredskap (TIB). Det finns heller inte en samlad bild kring vilken beredskap nämnder/förvaltningar har i form av alternativ tillgång till information eller alternativa arbetssätt.

Som alla kommuner har Skara hanterat tillbud och kriser tidigare men då mer adhoc. Vid ett IT-avbrott finns ingen formaliserad rutin för hur man ska agera och vem som ska kontaktas. Dock finns dokument/rutiner för avvikelsehantering och incidentrapportering. Inom ramen för V6 finns dokument där kritiska system och områden listats. De viktigaste områdena för en kommun anses vara el, vatten och omsorg. Hur detta relaterar till kommunens kravställning mot Göliska är oklart.

De brister som finns i dagsläget skulle kunna leda till att information hamnar fel med stora konsekvenser som följd.

De alternativa arbetssätt som finns på plats beskrivs som följande av de vi intervjuat. Om telefonin går ned ska invånarna ändå kunna kontakta kontaktcenter. Kommunikationsavdelningen har förtryckta affischer som man kan sätta upp för att nå ut. Det finns även kriskommunikationshandböcker upptryckta, även lokalmedia/lokalradio kan användas för att nå ut. Om ett längre IT-avbrott skulle inträffa finns larmkort som delats ut till medarbetarna.

Vi har inte kunnat få en fullständig eller heltäckande bild av vilka åtgärder som är tänkta vidtas eller vilka alternativa arbetssätt som finns förberedda. Detta pga att det i dagsläget inte finns en heltäckande beskrivning över vilken beredskap som finns i resp förvaltning/nämnd. Kommunen bedöms därför ha brister i sin beredskap inför ett längre IT-avbrott. Det finns även brister i det nuvarande arbetet med informationssäkerhet. Vi anser det dock positivt att kommunen tagit steg för att förbättra och stärka arbetet och den faktiska informationssäkerheten. Viktigt att kommunen och kommunstyrelsen agerar för att komma till rätta med de brister som finns i dagsläget.

Har kommunen kartlagt vilka effekter ett avbrott skulle få på den dagliga verksamheten, tex på trygghetslarm?

Kommentar och bedömning

Bilden kring vilka effekter ett avbrott skulle kunna få på den dagliga verksamheten skiljer sig åt mellan de som intervjuats. Då kraven är höga på tillgänglighet och säkerhet i kommunikation och information skulle ett längre avbrott rörande el eller IT påverka kommunens verksamhet. I dagsläget finns det inte någon kartläggning av vilka effekterna skulle bli. Vilka effekter ett avbrott skulle kunna få bör klarläggas. Detta så att kommunen och kommunstyrelsen vet vilka risker som kräver åtgärder för att minimera effekterna av ett större avbrott. Vid intervjuerna framkommer att omsorgen borde ha alternativa rutiner på plats för att hantera mediciner etc men ingen av de vi intervjuat vet med säkerhet hur dessa rutiner ser ut.

Kommunens ledning menar att effekterna av en IT-krasch vore att kommunen inte kan utföra de mest basala uppdragen rörande liv och säkerhet. Kommunen behöver se över att rätt åtgärder kommer på plats. I budgeten 2022 har kommunstyrelsen till nämnderna uppdragit att de ska se på erfarenheter och

lärdomar kring Covid. Det upplevs också finnas ett motsatsförhållande mellan säkerhet och öppenhet. Öppenheten behöver också värnas av kommunen.

I övrigt tas upp att effekterna av en IT-krasch upplevs som oklara i dagsläget. Men också att om en krasch inträffar så kan mycket av kommunens verksamhet förskjutas något tidsmässigt utan att det skulle leda till allvarliga konsekvenser. Arbete rörande liv och hälsa behöver dock alltid genomföras.

Vad gäller trygghetslarm anges att det finns rutiner i händelse av ett avbrott, tanken är att gå över till manuell övervakning. Detta kräver dock att man får relevant information från leverantören om att larmet inte hörs och därmed inte fungerar. Även om krav om detta ställs i upphandling kräver det att leverantören lever upp till sina åtaganden. Kommunen bör se över om de åtgärder som görs i dagsläget är tillräckliga för att trygga larmens funktion.

Ett IT-avbrott skulle leda till att det blir svårt få ut information både internt/externt. Omsorgen skulle inte kunna komma åt journaler etc. Den viktigaste lärdomen utifrån inträffade händelser är dock att informationssäkerhetsfrågan fick utrymme och att ledningen fick upp ögonen för detta.

De stora utmaningarna för kommunen beskrivs i dagsläget som hur väl lagkrav uppfylls idag. Förstår kommunen och ledningen konsekvenserna av om system ligger nere? Pga pandemin har det varit få övningar. Att det finns en beredskap och heltäckande bild av vilka effekter ett avbrott skulle få är viktigt för kommunens beredskap och givetvis för den faktiska informationssäkerheten.

För att minimera effekterna vid ett avbrott behövs en tydlig planering och tydlig ansvarsfördelning. Kommunen och kommunstyrelsen behöver förbättra arbetet kring informationssäkerhet för att nå dit. Även om delar av kommunens arbete kan skjutas på framtiden så behöver kommunen/kommunstyrelsen agera för att minimera effekterna av en ev IT-krasch.

Har kommunen ställt tillräckliga krav på sin IT-leverantör?

Kommentar och bedömning

Det finns ett avtal och diverse forum för kommundirektörer där VD och Göliska träffas 4 ggr/år. Dock verkar innehållet i dessa möten inte främst vara informationssäkerhet utan andra frågor. I dagsläget finns ingen tydlig eller uppdaterad prioritering av systemen i form av vilka som är viktigast och ska vara igång först vid ett avbrott. Det är också otydligt vilken del Göliska spelar i kommunens arbete med informationssäkerhet och hur parterna samverkar för att hålla en god informationssäkerhet. Det finns oklarheter i vilka krav som ställs kring informationssäkerhet på Göliska. Intervjupersonerna upplever det som otydligt vilket ansvar det innebär att ha ett system och vara systemägare. Då kommunen i och med bildandet av Göliska tappade IT-kompetens upplevs det som svårt driva informationssäkerhetsarbetet och upprätthålla en god dialog med Göliska kring detta ämne.

För att alla samarbeten ska fungera och ett bra arbete med informationssäkerhet ska komma på plats behöver kommunen och kommunstyrelsen hantera frågan från grunden och ge stöd till förvaltningarna för att få ett fungerande arbete och kravställning mot leverantör.

Under intervjuerna uppkommer flera synpunkter att avtalet med Göliska och kommunens ledning av och arbete med informationssäkerhet behöver förbättras. Arbetet bör göras mer konkret och inledningsvis inriktas på att få en överblick över läget och förutsättningarna. Kompetensfrågan och

ansvars/uppgiftsfördelning mellan kommunen och Göliska behöver klarläggas. Kopplingen och dialogen behöver stärkas vilket kräver att kommunen får en ökad kompetens för att kunna driva arbetet framåt på ett ändamålsenligt sätt. Att dessa förutsättningar finns är mycket viktigt för att kunna hålla en god informationssäkerhet i praktiken. Kommunstyrelsen bör agera för att få dessa förutsättningar på plats.

Vilken återkoppling lämnas till kommunstyrelsen angående informationssäkerhetens status och vilka åtgärder vidtas?

Kommentar och bedömning

Före 2021/22 var det i princip ingen återkoppling till kommunstyrelsen gällande informationssäkerhetens status och vilka åtgärder som vidtas. Nuvarande kommundirektör informerar om vikten av informationssäkerhet och ev incidenter. Det är främst vid stora fel som information tas upp med kommunstyrelsen. Pga att kommunen inte har något LIS etablerat har kommunstyrelsen inte fått någon återkoppling om det faktiska läget/tillståndet kring informationssäkerheten i kommunen. Kommunens chefsledningsgrupp får dock löpande information från Göliska men återrapporteringen om status etc har dock varit svagare. Den lägesgenomgång som gjordes av informationssäkerheten 2017 nådde aldrig fram till kommunstyrelsen. Återkopplingen till kommunstyrelsen behöver förbättras.

Vi anser att det är mycket viktigt att kommunstyrelsen visar sitt fortsatta engagemang för informationssäkerhetsfrågor då dessa frågor är vitala för en väl fungerande kommun. Vikten av att kommunstyrelsen och kommunens ledning tydligt visar engagemang för informationssäkerheten framkom vid alla intervjuer. Kommunstyrelsen bör också driva på arbetet med att få ett ledningens informationssystem på plats. Detta så att kommunstyrelsen och kommunens chefer kan få en överblick över vilken status informationssäkerheten har i Skara kommun. Dessutom bör uppföljning och status på informationssäkerhet införas som en del av kommunstyrelsens uppsiktsplikt. Det arbete som påbörjats är en god grund men kräver ett långsiktigt och kontinuerligt engagemang.

Deloitte.