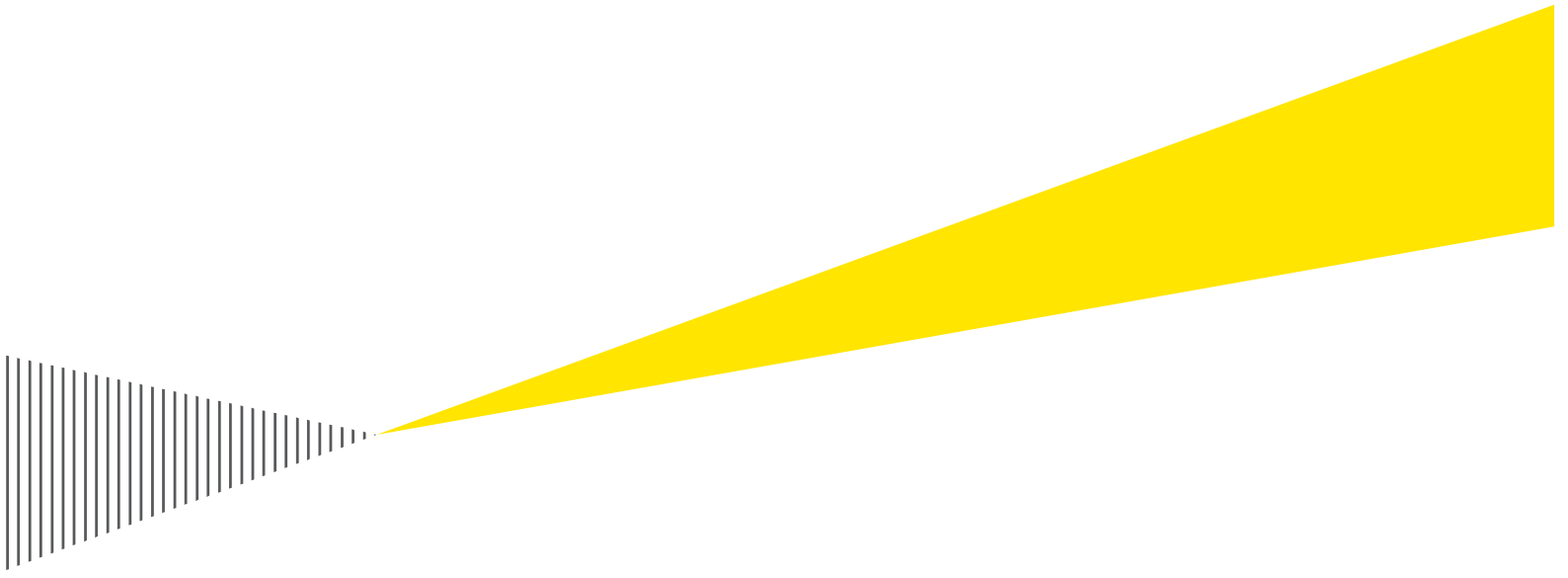
Revisionsrapport 2020
Genomförd på uppdrag av revisorerna
augusti 2020

Stenungsunds kommun

Granskning av IT- och informationssäkerhet



Building a better working world

Innehållsförteckning

Sammanfattning

De förtroendevalda revisorerna i Stenungsunds kommun har beslutat att genomföra en granskning i syfte att kartlägga kommunens arbete med IT- och informationssäkerhet samt ansvarsfördelningen mellan kommunen och SOLTAK gällande IT- och informationssäkerhetsarbetet. EY har ombetts att granska om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med IT- och informationssäkerhet är ändamålsenligt, samt bedöma vilka processer som idag finns för att säkerställa och följa upp att tillräcklig IT-säkerhet upprätthålls hos SOLTAK.

Baserat på genomförd granskning har arbetet med att upprätta mer detaljerade avtal med SOLTAK och formulera och följa upp behov relaterat till IT- och informationssäkerhet identifierats som ett av de främsta förbättringsområdena för Stenungsunds kommun. Nedan följer de mest väsentliga slutsatserna:

- Det avtal som kommunen upprättat med SOLTAK uppges vara under omarbetning, men är vid tidpunkten för granskningen skrivet på övergripande nivå. Kommunen har i detta inte specificerat några detaljerade krav vad gäller arbetet med IT- och informationssäkerhet, vilket kan påverka kommunens möjlighet att kravställa och följa upp på den faktiska tjänsteleveransen.
- Vid tidpunkten för granskningen finns inte heller någon beslutad process för uppföljning och återrapportering för de tjänster som SOLTAK levererar inom tjänsteområde IT, och det sker därför inte heller någon strukturerad uppföljning av SOLTAKs arbete med avseende på IT- och informationssäkerhet. Historiskt sett har det inte kommunicerats någon kravställning från kommunens sida inom tjänsteområde IT, varför uppföljningsarbetet i nuläget inte sker på ett strukturerat och ändamålsenligt sätt.
- Vidare arbetar kommunen i nuläget inte i enlighet med något ledningssystem för informationssäkerhet och det arbete som utförs internt sker inte alltid systematiskt. På så sätt saknar man en tydlig intern organisation vilken kan agera motpart och kravställare gentemot SOLTAK i det löpande arbetet med informationssäkerhetsrelaterade frågor.
- Kommunen har startat ett internt arbete inom området genom exempelvis informationsklassning och riskanalyser men vid tidpunkten för granskningen har detta arbete ännu inte lagt grunden för välavvägd kravställning gentemot SOLTAK. Därför är tjänsteleveransen och de servicenivåer som levereras av SOLTAK inte grundade i någon analys av kommunens verksamheters faktiska behov.

Mognadsnivån i kommunens arbete med informationssäkerhet med avseende på samarbetet mellan kommunen och SOLTAK bedöms generellt vara låg till medelgod. Avsaknaden av tydlig ansvarsfördelning och styrning har historiskt varit en bidragande faktor till att kommunen haft bristande möjlighet kravställa och följa upp på SOLTAKs tjänsteleverans. Med bakgrund i flertalet pågående initiativ som omarbetning av avtal och tjänstebeskrivningar samt tydliggörande av ansvar och organisation hos SOLTAK bedöms dock Stenungsunds kommun ha goda förutsättningar för att på både kort och lång sikt bedriva ett ändamålsenligt arbete med IT- och informationssäkerhet i samarbetet med SOLTAK.

1.1. Bakgrund

Stenungsunds kommun 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 att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

Kommunens revisorer har identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet, samt ett behov av översyn av ansvarsfördelningen mellan kommunen och SOLTAK gällande IT- och informationssäkerhetsarbetet. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte specifikt relaterade till Stenungsunds kommun utan gäller hela den offentliga sektorn.

1.2. Syfte

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med IT- och informationssäkerhet är ändamålsenligt, samt att bedöma vilka processer som idag finns för att säkerställa och följa upp att adekvat IT-säkerhet upprätthålls hos SOLTAK.

1.3. Revisionskriterier

Granskning har genomförts enligt god revisionssed inom informationssäkerhetsområdet. Granskningen är gjord mot Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk LIS, som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.

1.4. Revisionsfrågor

- Efterlever SOLTAK det avtal man har med kommunen avseende IT-säkerhet? Och styr SOLTAK IT-säkerheten för Stenungsunds kommun i enlighet med god praxis?
- Genomför kommunen kontinuerlig och ändamålsenlig uppföljning av IT-säkerheten hos SOLTAK?

1.5. Avgränsning

Granskningen är avgränsad till att ge en övergripande bild av området och kan i första hand användas till att utgöra en lägesbild och kunskapsunderlag i det fortsatta IT- och informationssäkerhetsarbetet. Granskningen avgränsas i enlighet med avsnitt 1.4 Revisionsfrågor. Granskningen fokuserar således på det arbete som avtalats med och utförs av SOLTAK samt kommunens uppföljning av detta, och därmed behandlas inte kommunens interna informationssäkerhetsarbete i denna rapport utom där det har direkt betydelse för samarbetet med SOLTAK. I enlighet med detta fokuserar granskningen inte heller på det IT- och informationssäkerhetsarbete som utförs av SOLTAK där detta faller utanför ramarna för vad kommunen kravställt på i gällande avtal.

1.6. Metod och genomförande

Granskningen genomfördes under maj och juni 2020 genom studier av styrdokument och intervjuer med berörda funktioner med nyckelroller inom kommunens IT- och informationssäkerhetsarbete samt nyckelpersoner hos SOLTAK. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet.

Information kring områdena insamlas både genom granskning av relevanta dokument, samt genom att EY:s specialister genomför granskningsmöten med relevanta personalkategorier i kommunen. Dokument som inhämtas är framförallt styrdokument som policy, ansvarsfördelning, riktlinjer och rutiner avseende informations- och IT-säkerhet, IT-driftsäkerhet, intern kontroll samt bevis av beslut och arbetsfördelning.

Intervjufrågor har utarbetats utifrån syftet och revisionsfrågorna. Frågorna är anpassade efter intervjupersonernas olika roller och ansvar och förteckning över intervjuade funktioner samt erhållna dokument framgår av Bilaga 1. Intervjuade representanter från kommunen och SOLTAK har getts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Som avtalats i uppdragsbrevet har granskningen även kvalitetssäkrats internt av EY.

2. Svar på revisionsfrågor

Granskningen har syftat till att på uppdrag av revisorerna genomföra en övergripande genomgång av kommunens informationssäkerhetsarbete med fokus på samarbetet med SOLTAK. Granskningen har utgått från två revisionsfrågor, vilka besvaras nedan.

Efterlever SOLTAK det avtal man har med kommunen avseende IT-säkerhet? Och styr SOLTAK IT-säkerheten för Stenungsund kommun i enlighet med god praxis?

Det avtal som Stenungsunds kommun upprättat med SOLTAK är skrivet på övergripande nivå och kommunen har i detta inte specificerat några detaljerade krav vad gäller arbetet med IT- och informationssäkerhet. Detta kan leda till risk för bristande möjlighet att styra och följa upp på de tjänster som levereras av SOLTAK, på grund av att det saknas överenskommelser och avtal som till exempel tydliggör ansvarsfördelning och kvalitetsmått. SOLTAK bedöms dock, för de områden som specifikt avtalats, efterleva det avtal man har med kommunen och styra IT-säkerheten i enlighet med god praxis. För SOLTAKs egna systemstöd finns också väl utvecklade riktlinjer och instruktioner för kritiska informationssäkerhetsaktiviteter, både i individuella system och för systemövergripande aktiviteter.

Då gällande avtal mellan kommunen och SOLTAK inte reglerar krav på IT-säkerhet eller innehåller de IT-säkerhetsaspekter som enligt praxis bör inkluderas i avtal med en extern leverantör av IT-tjänster, visar denna granskning på flertalet risker kopplat till hur kommunen säkerställer ändamålsenlig IT-säkerhet utifrån gällande praxis inom IT-säkerhetsområdet.

Genomför kommunen kontinuerlig och ändamålsenlig uppföljning av IT-säkerheten hos SOLTAK?

Baserat på genomförd granskning har arbetet med kontinuerlig och ändamålsenlig uppföljning av IT-säkerheten identifierats som ett av kommunens främsta förbättringsområden. Kommunen arbetar inte efter någon fastställd process för uppföljning och återrapportering för de tjänster som SOLTAK levererar inom tjänsteområde IT, och därför sker inte heller någon strukturerad uppföljning av SOLTAKs leverans med fokus på IT- och informationssäkerhet. Ett antal samarbetsforum existerar och utvecklas löpande, men historiskt sett har man inom ramen för dessa inte fokuserat på kontinuerlig och ändamålsenlig uppföljning av IT- och informationssäkerhet specifikt. Vid tidpunkten för granskningen har inga bestämda parametrar eller nyckeltal för uppföljning eller återrapportering beslutats och ingen direkt kravställning har kommunicerats från kommunens sida inom tjänsteområde IT. Därför sker uppföljningsarbetet i nuläget inte sker på ett strukturerat och ändamålsenligt sätt.

Avsaknaden av olika former av avtal och överenskommelser, som lyfts ovan, medför enligt vår mening risker kopplat till kommunens styrning, uppföljning och kontroll av SOLTAK. Då det saknas konkret kravställning från Stenungsunds kommun vad gäller SOLTAKs IT- och informationssäkerhetsarbete, har detta identifierats som ett av kommunens främsta förbättringsområden.

3. Genomgång av granskade områden

3.1. Avtalade tjänster

I mars 2016 undertecknade kommunchef samt VD för SOLTAK *”Avtal mellan SOLTAK AB och Stenungsund kommun”* vilket utgör det huvudsakliga avtalet för samtliga områden SOLTAK levererar tjänster inom. Avtalet baserades på ett antal beslut tidigare fattade av kommunfullmäktige, som är relevanta för samarbetet. SOLTAK levererar tjänster till Stenungsunds kommun inom tre huvudsakliga områden vilka är ekonomiadministration, löneadministration, IT-drift och IT-support. I tillägg till dessa driver SOLTAK även individuella projekt för kommunen, vid exempelvis förändringar i de system som driftas. IT-drift och support är de tjänster med störst omfattning och specificeras i tjänstebeskrivningarna IT Arbetsplats, Nät och Datacenter. Tjänstebeskrivningarna är upprättade av SOLTAK och innehåller på hög nivå tjänstebeskrivning, specificerade servicenivåer, information kring underhållsaktiviteter samt priser.

Av huvudavtalet framgår att bolaget för tjänsteområde IT ska förvalta kommunernas befintliga IT-miljöer och erbjuda kommunernas verksamheter samma servicenivå som innan verksamhetsövergången till bolaget, för att sedan övergå till en kommungemensam IT-miljö. Utöver detta specificerar inte avtalet ansvarsfördelning vad gäller IT- eller informationssäkerhet. Vid tidpunkten för granskningen finns inga ytterligare, mer detaljerade avtal utöver de tjänstebeskrivningar som upprättats av SOLTAK själva. Avtalsstrukturen är dock under omarbetning och den nya versionen med tillhörande underavtal planeras innehålla mer specifik kravställning vad gäller informationssäkerhet.

3.2. Organisation

Stenungsunds kommuns digitaliseringschef är huvudsaklig kontaktperson gentemot SOLTAK och företrädare för kommunen vad gäller IT-relaterade frågor. Digitaliseringschefen har dock inget informationssäkerhetsansvar internt. Istället agerar kommunens säkerhetssamordnare även informationssäkerhetssamordnare för det interna arbetet, och ansvarar för kontakten med kommunens systemförvaltarorganisation i dessa frågor. Arbetet med att systematiskt arbeta med informationssäkerhet tillsammans med systemförvaltarorganisationen är relativt nystartat och informationsklassning och riskanalyser för kommunens verksamhetssystem är pågående. Inom ramen för arbetet med att kartlägga känslig information i kommunens verksamhetssystem uppger kommunen att man ställt ett antal frågor till SOLTAK kring säkerhet i driftsmiljön, men att dessa frågor inte besvarats av SOLTAK. Med anledning av detta har informationsklassningen inte kunnat slutföras i de system som driftas av SOLTAK, och resultaten har därför inte heller legat till grund för någon kravställning gentemot SOLTAK. Vad gäller intern styrdokumentation har kommunen upprättat övergripande IT- och informationssäkerhetspolicys vilka är daterade 2006. Dessa kompletteras med säkerhetsinstruktioner, som vid tidpunkten för granskningen reviderats senast 2003. All information som lagras och hanteras av SOLTAK på uppdrag av kommunen ägs av kommunen och dess verksamheter, dock görs verksamhetens information tillgänglig för SOLTAK inom ramen för tjänsteleveransen. SOLTAK omfattas inte av kommunens interna styrdokumentation utan samarbetet styrs i egenskap av extern leverantör av de avtal som upprättats mellan parterna. Vid tidpunkten för granskningen har SOLTAK inte upprättat någon intern styrdokumentation såsom informationssäkerhetspolicy eller säkerhetsinstruktioner, utöver det som krävs av upprättade avtal. Stenungsunds kommun uppger dock att man kommunicerat uttryckligt önskemål till SOLTAK angående upprättande av IT- och informationssäkerhetspolicy.

Inom ramen för tjänsteområdena ekonomi och lön äger SOLTAK själva det systemstöd som används och ansvarar därför för förvaltning och operativa rutiner för dessa system. Här finns väl utvecklade riktlinjer och instruktioner för kritiska informationssäkerhetsaktiviteter såsom behörighetshantering, och man har även systemövergripande rutiner för exempelvis förändringshantering, incidenthantering, backup och återläsning. Utöver detta sköter SOLTAK driften för 50-talet system för Stenungsunds kommun. För varje sådant system finns utsedd systemägare vilken oftast är en chef på kommunen, samt en systemförvaltare i verksamheten. Hos SOLTAK finns teknisk systemförvaltare utsedd för respektive system.

3.3. Samarbetsforum

Stenungsunds kommun och SOLTAK har fyra olika typer av samarbetsforum där man sammanträder på regelbunden basis:

- Kundråd IT
- Driftmöten
- UB-möten (Uppdragsbeställningar, för uppdrag som faller utanför ramen för ordinarie tjänsteleverans)
- CAB-möten (Change Advisory Board, för förandringshantering)

Ovan samarbetsforum är möten där Stenungsunds kommun sammanträder med representanter från SOLTAK samt i vissa fall representanter från övriga ägarkommuner. Kundråd IT är ett möte med strategiskt fokus där deltagarna diskuterar kommunövergripande, mer långsiktiga och strategiska frågor. Detta kan till exempel avse förslag till nya tjänster, leverans- och serviceuppföljning samt behov av gemensamma investeringar. Ägarkommunerna har nyligen infört ett förmöte till kundråd IT för att gemensamt förbereda sig och enas om viktiga frågor, och möjlighet finns även att vid behov hålla kommunspecifika kundråd där man endast diskuterar frågor rörande en kommun. Driftmötena har ett operativt fokus där de följer upp på leveransrelaterade frågor som hantering av ärendeloggar, vilket historiskt har varit viktigt då man upplevt problem med lång handläggningstid för ärenden. UB-möten är i sin tur forum där man löpande diskuterar uppdrag som utförs av SOLTAK utanför ordinarie tjänsteleverans och för vilka kommunen måste lägga en separat uppdragsbeställning. Under dessa möten sker uppföljning och prioritering av dessa beställningar. Slutligen utgör CAB-möten det forum förändringshantering diskuteras.

3.4. IT- och informationssäkerhetsrutiner

Som tidigare nämnts behandlar de avtal som upprättats mellan Stenungsunds kommun och SOLTAK inte ansvar för eller kravställning inom informationssäkerhet specifikt. De tjänstebeskrivningar som SOLTAK upprättat för respektive tjänsteområde inom IT, det vill säga IT-arbetsplats, Nät samt Datacenter, innefattar dock viktiga säkerhetsaspekter inom respektive område såsom ansvarsfördelning för utveckling, förvaltning, drift och underhåll, gällande servicenivåer och processer, virusskydd och dylikt. Utöver detta finns hos SOLTAK ytterligare dokumentation kring rutiner för backup, återläsning och övervakning, samt mer detaljerade processbeskrivningar för förändrings- och incidenthantering.

För utveckling i de system där SOLTAK ansvarar för driften finns en dokumenterad process för förändringshantering. Processen beskriver övergripande roller och ansvarsfördelning mellan kommunen i egenskap av beställare och SOLTAK i egenskap av utförare. Processen för förändringshantering startar genom att det antingen från kommunens eller SOLTAKs sida inkommer en förfrågan om förändring (RFC). Varje förfrågan diskuteras och beslutas om i CAB-möten där samtliga kommuner är representerade. Underlag till CAB-möten skickas ut

som förberedelse så att varje kommun skall ha möjlighet att i förväg utvärdera förfrågan om förändring. Efter godkänt beslut har kommunerna ingen formell medverkan i själva verkställandet av en förändring, vilket genomförs av SOLTAK, utan tar i många fall endast del av en stängningsrapport för den enskilda förändringen efter att den genomförts. Undantagsfall har funnits vad gäller särskilt stora uppgraderingar där kommunen varit aktivt involverade i själva utvecklings- och testprocessen. Stenungsunds kommun har begärt att få ta en mer aktiv roll i större förändringsprojekt genom att medverka i projektens styrgrupp, men det uppges att detta hittills endast skett sporadiskt och inte systematiskt. Vidare är test- och produktionsmiljöerna segregerade för SOLTAKs internt ägda system, och för kommunens egna system uppges att SOLTAK har möjlighet att sätta upp separat testmiljö som så efterfrågas av kommunen.

Processen för incidenthantering har enligt kommunen historiskt sett inte varit tydligt formulerad eller dokumenterad, vilket i många fall påverkat hanteringen under incidentlivscykeln. Dock uppges att betydande förbättringar vad gäller själva hanteringsprocessen skett i närtid. När en incident inträffar finns en process upprättad hos SOLTAK där kommunen är involverad, och både kommunen och SOLTAK uppger att processen i nuläget fungerar bra och att rapporteringsvägar och ansvarsfördelning med utsedd incidentansvarig finns. Hos kommunen finns utsedda kontaktpersoner som ansvarar för initial bedömning och för att se till att kommunikation till berörda sker där det bedöms nödvändigt. Ansvarig hos SOLTAK genomför sedan kontinuerlig uppföljning kring incidenten och kommunen är i regel involverad genom hela processen från rapportering till stängning. Det uppges dock att detta oftast sker på en övergripande nivå och att uppföljningen inte fokuserar på de faktiska åtgärder som tekniskt vidtas. Efter att en incident slutligen stängts och slutrapporterats uppger kommunen att det inte sker någon strukturerad uppföljning eller återkoppling i syfte att analysera incidenten och dess orsaker.

För upphandling av nya system har SOLTAK tidigare agerat rådgivande till kommunen när detta behövts, men har i övrigt inte haft någon aktiv roll i upphandlingsprocessen. Stenungsunds kommun arbetar med att ta fram en ny process och rutin för upphandling av verksamhetssystem där man har för avsikt att involvera SOLTAK i större utsträckning för att på så sätt se till att man arbetar med korrekt kravställning så tidig som möjligt. Processen är inte fastställd vid tidpunkten för granskningen utan håller på att testas, men SOLTAK är informerade om att de önskas ta en mer aktiv roll tidigt i upphandlingen. Processen syftar till att utgöra underlag vid leverantörsdialoger och behandlar viktiga aspekter inom IT- och informationssäkerhet vilket ska underlätta för kommunen att arbeta fram en korrekt kravställning gentemot nya leverantörer. Exempel på områden som inkluderas är personuppgiftshantering i enlighet med Dataskyddsförordningen, ledningssystem/metodik för informationssäkerhet, åtkomstrutiner och incidenthantering och dylikt.

Det finns ett avtal mellan Stenungsund kommun och SOLTAK för hyra av serverhall, denna serverhall används av SOLTAK för deras datacenter. Inför tecknandet av detta avtal 2017 genomförde Stenungsunds kommun och SOLTAK en risk- och sårbarhetsanalys i syfte att säkerställa att tillräcklig fysisk säkerhet upprätthålls. 12 sårbarheter och risker identifierades och en åtgärdsplan för upprättades gemensamt. Främst identifierades risker inom området behörighet och åtgärder såsom förbättrade lås och larmfunktioner och rutiner för säkerhetsklassning av personal beslutades. Det avtal som sedan slöts beskriver i detalj ansvarsfördelningen mellan kommunen och SOLTAK vad gäller säkerhet kring serverhallen. Ansvaret för att upprätthålla ändamålsenliga rutiner i relation till de potentiella risker som lyftes i utförd analys har särskilt beskrivits.

3.5. Personuppgiftshantering

Inför införandet av Dataskyddsförordningen 2018 genomförde kommunen ett grundligt arbete i syfte att kartlägga sin personuppgiftshantering och förbereda sig för den nya lagstiftningen. Kommunen anställde ett Dataskyddsombud som ledde projektet inför övergången till Dataskyddsförordningen, denne ansvarade även för framtagande av dokumentation samt för att informera och utbilda kommunens personal. Dataskyddsombudet har dock lämnat sin tjänst i kommunen och istället har kommunjuristen tillfälligt förordnats ansvaret. Vid tidpunkten för granskningen har kommunen tecknat avtal med Göteborgsregionens kommunalförbund om gemensamt Dataskyddsombud gällande med start 2020-08-10.

Inom ramen för införandeprojektet inventerades samtliga av kommunens verksamhetssystem där personuppgifter hanteras. För de personuppgiftsbehandlingar som förekommer i de verksamhetssystem och IT-lösningar kommunen använder har ett elektroniskt register upprättats i enlighet med dataskyddsförordningen. Som tidigare nämnts har kommunen internt inte färdigställt informationsklassning och riskanalys av de egna systemen, och inga informationsklassificeringar eller konsekvensbedömningar har genomförts gemensamt mellan kommunen och SOLTAK ännu. SOLTAK har dock genomfört inventering och upprättat förteckning över de personuppgifter som behandlas i de egna systemen.

Kommunens Dataskyddsombud tog fram ett nytt personuppgiftsbiträdesavtal för externa leverantörer, vilket även tecknats med SOLTAK. Då SOLTAK levererar tjänster till flertalet kommuner uppges att arbetet med att nå ett godkänt avtal tog tid och det avtal som tecknats är daterat till november 2019. Avtalet omfattar viktiga aspekter såsom ansvarsfördelning, säkerhetsåtgärder, sekretesskrav och revisionskrav och -rättigheter, dock har någon intern revision eller granskning från kommunens sida ännu inte genomförts, då avtalet är så pass nytecknat.

4. Iakttagelser och rekommendationer

Under granskningen har EY identifierat iakttagelser relaterat till revisionsfrågorna. För varje iakttagelse har EY lämnat rekommendationer som syftar till att stödja Stenungsund kommun i dess framtida samarbete med SOLTAK med avseende på IT- och informationssäkerhet. De av EY identifierade iakttagelserna har klassificerats enligt tre prioriteringsnivåer:

	**Prioritering kort sikt**: Observation som bör hanteras på kort sikt. Anses kunna ha hög påverkan på verksamhetens mål, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.
	**Prioritering medellång sikt:** Observation som bör hanteras på medellång sikt. Anses kunna ha påverkan på verksamhetens mål, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.
	Prioritering lång sikt: Observation som kan hanteras på längre sikt. Påverkar ej direkt verksamhetens mål, men som kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

4.1. Stenungsunds kommun har inte specificerat krav på IT- och informationssäkerhets i avtalet med SOLTAK

Observation
Prioritering
Kort sikt

Det avtal som Stenungsunds kommun upprättat med SOLTAK är skrivet på övergripande nivå och kommunen har i detta inte specificerat några detaljerade krav vad gäller arbetet med IT- och informationssäkerhet. Det saknas därför konkret kravställning från Stenungsunds kommun gentemot SOLTAK vad gäller dess IT- och informationssäkerhetsarbete. Avtal med extern leverantör av IT-tjänster bör enligt praxis minst omfatta krav på informationssäkerhetspolicy och övriga styrdokument, IT-säkerhetsrutiner i produktionsmiljö, incidenthantering, kommunikation och tillgänglighet, krav på konfidentialitet, behörighetskrav, kontinuitetsplanering och tillhörande tester, åtkomst till process-beskrivningar samt revisionsrättigheter och liknande. Avsaknad av sådana avtal innebär att kommunen i egenskap av beställare inte har någon konkret överenskommelse att ställa eventuella avvikelser och problem med leverantörens tjänster emot och begränsar möjligheten för kommunen att kravställa och följa upp på SOLTAKs arbete. Att inte upprätta detaljerade avtal med en extern leverantör av tjänster som beskriver ansvarsförhållanden och gränsdragning mellan beställare och leverantör medför därför en risk för att beställaren inte erhåller de tjänster och det stöd man faktiskt betalar för och att dess verksamheter i längden kan ta skada.

Rekommendation

Vi rekommenderar kommunstyrelsen att:

1. Genomföra en analys av kommunens och dess verksamheters faktiska behov utifrån IT- och informationssäkerhet. Denna analys bör föregås av informationsklassning och riskanalys, se vidare iakttagelse 3.2.
2. Inom ramen för nuvarande omarbetning av avtal och tjänstebeskrivningar, inkludera kravställning inom särskilt viktiga informationssäkerhetsaspekter.
3. Tillse att kommande upphandlingsinstruktion detaljerar viktiga kravställningar som skall genomgås när avtal tecknas med ny IT-leverantör. Denna kan således utgöra en bra grund för omarbetning av kommunens avtal med SOLTAK i egenskap av driftleverantör.

Arbetet med att specificera detta kan med fördel också genomföras tillsammans med respektive tjänsteägare som ska tillsättas hos SOLTAK, för att på så sätt utforma både avtal samt tjänstebeskrivningar vilka är väl grundade och praktiskt gångbara.

4.2. Stenungsunds kommun har inte grundat kravställningen gentemot SOLTAK i fråga om IT-och informationssäkerhet i verksamhetens faktiska behov

I nuläget har kommunen inte implementerat något ledningssystem för informationssäkerhet och det arbete som utförs internt sker i vissa avseenden inte systematiskt. På så sätt saknar man en tydlig intern organisation vilken kan agera motpart och kravställare gentemot SOLTAK i det löpande arbetet med informationssäkerhetsrelaterade

frågor. Då kommunens interna arbete inom området såsom med informationsklassning och riskanalyser är relativt nyligen påbörjat har man ännu inte kommit till det skedet när detta kan mynna ut i en mer välavvägd kravställning gentemot SOLTAK. Därför är tjänsteleveransen och de servicenivåer som levereras av SOLTAK inom ramen för dessa inte baserade på någon analys av kommunens verksamheters faktiska behov. En sådan analys är en förutsättning för kommunen för att kunna säkerställa att verksamheten får det stöd den behöver i tillräckligt god tid och till rätt kostnad. Att inte avtala tjänstenivåer med grund i verksamheternas faktiska behov kan resultera i att verksamheten lider skada då beställaren inte får den support eller service beställaren behöver för att kunna bedriva verksamheten på ett avbrottsfritt och tillfredsställande sätt. Det kan även resultera i att verksamheten riskerar erhålla onödigt hög nivå av support till en högre kostnad än nödvändigt.

Observation
Prioritering
Kort sikt

Kommunstyrelsen rekommenderas att:

1. Se över kommunens interna informationssäkerhetsarbete i syfte att säkerställa att detta bedrivs på ett systematiskt sätt och kan utgöra grund för kravställning gentemot SOLTAK och dess tjänsteleverans inom IT.
2. Se till att arbetet med att systematiskt genomföra informationsklassning och riskanalys av verksamhetens IT-system fullföljs. Vi rekommenderar även kommunstyrelsen att säkerställa att dessa resultat används som underlag för att utveckla kravställningen gentemot SOLTAK samt att tjänstenivåer anpassas utefter respektive verksamheters unika behov där detta bedöms vara nödvändigt.
3. Vi rekommenderar även att se över möjligheten att tydliggöra målbilden med informationssäkerhetsarbetet och definiera en intern organisation vilka arbetar upp kontaktytor hos SOLTAK vad gäller informationssäkerhetsfrågor specifikt, förslagsvis genom att dra nytta av den nya avtals- och ansvarsstrukturen vilken är under uppbyggnad. Detta för att möjliggöra bättre förutsättningar för kommunen att kravställa dels gentemot SOLTAK, men även mot andra leverantörer av IT-system.

Rekommendation

4.3. Det saknas strukturerad uppföljning av SOLTAKs tjänsteleveranser inom IT

Kommunen har inte arbetat fram någon specifik process för uppföljning och återrapportering i relation till de tjänster som SOLTAK levererar inom tjänsteområde IT, och därför sker inte heller någon strukturerad uppföljning av SOLTAKs leverans relaterat till IT- och informationssäkerhet. I de samarbetsforum som finns, såsom kundråd IT och driftmöten, har fokus historiskt sett i till stor del legat på att i första hand följa upp på och stänga försenade ärenden och att diskutera övergripande SLA-komponenter och kostnader. Inga bestämda parametrar för uppföljning eller återrapportering har beslutats trots att frågan kring vilken typ av statistik som skulle kunna vara relevant har varit uppe för diskussion inom ramen för dessa forum. Inom de övriga tjänsteområdena Lön och Ekonomi har konkreta nyckeltal framtagits för vilken löpande uppföljning och

Observation
Prioritering
Medellång

återrapportering sker, dock har ingen sådan kravställning kommunicerats från kommunens sida inom tjänsteområde IT, varför uppföljningsarbetet i nuläget inte sker på ett strukturerat och ändamålsenligt sätt. Avsaknad av en process för uppföljning av servicenivåer och andra relevanta parametrar innebär risk för att kommunen inte erhåller den nivå på leverans som avtalats och kan resultera i hinder mot att bedriva verksamheten på ett avbrottsfritt och tillfredsställande sätt.

Rekommendation

Kommunstyrelsen rekommenderas att:

1. Tillse att kommunen specificerar vilken information de vill ha återrapporterat från SOLTAK inom tjänsteområde IT, samt hur och med vilken frekvens detta ska ske. En standardiserad process för uppföljning och återrapportering är viktig för att säkerställa att kvaliteten bibehålls på en hög nivå och levereras i linje med de förväntningar och krav kommunen har på leveransen från SOLTAK. Vidare möjliggör en kontinuerlig återrapportering skyndsam identifiering av potentiella problem och ökad förmåga att lösa sådana problem med minsta möjliga påverkan på verksamheten.

4.4. Det saknas en process för utvärdering av incidenter mellan SOLTAK och Stenungsunds kommun

Observation
Prioritering
Lång sikt

För att kunna bedriva ett systematiskt arbete med incidenthantering bör kontinuerlig och gemensam utvärdering i inlärningssyfte genomföras. När en incident hanteras av SOLTAK å kommunens vägnar sker i många fall kontinuerlig kommunikation fram till att denna stängs då en incidentrapport levereras. Inget vidare arbete sker dock efter det att incidenten har stängts i syfte att utvärdera och lära av incidenten, dess orsaker och det arbete som gjorts för att kunna stänga denna och på så sätt uppnå kunskaps- och erfarenhetsutbyte. Att kommunen skapar förståelse kring orsaker och aktiviteter som gjorts för att lösa incidenten är viktigt i utbildningssyfte och kan bidra till att motverka att liknande incidenter inträffar igen, alternativt att inträffade incidenter får mindre påverkan.

Rekommendation

Kommunstyrelsen rekommenderas att

1. Tillse att kommunen arbetar fram en process för utvärdering och uppföljning av inträffade incidenter, i syfte att uppnå kunskaps- och erfarenhetsutbyte och således minska risken för att liknande incidenter inträffar eller får allvarlig påverkan i fortsättningen. Detta kan med fördel göras tillsammans med de tilltänkta tjänsteområdesansvariga på SOLTAK och tas upp som en agendapunkt inom ramen för något av de samarbetsforum som finns.

4.5. Stenungsund kommun är ej tillräckligt involverade i processen för förändringshantering

Observation
Prioritering
Lång sikt

Stenungsunds kommun är i egenskap av kund involverade i det initiala skedet av processen för förändringshantering där man efterfrågar förändringar samt godkänner huruvida en förändring ska genomföras eller ej. Detta uppges fungera väl för mindre förändringar i befintlig IT-miljö, dock saknas i synnerhet för större förändringar tydlig struktur för hur kommunen ska involveras i resterande delar av processen för förändringshantering, omfattande utveckling, test och produktionssättning samt nödvändiga beslut i relation till dessa aktiviteter. Vidare är test- och produktionsmiljöerna för SOLTAKs internt ägda system segregerade, och för kommunens egna system uppger SOLTAK att möjlighet finns att sätta upp separat testmiljö som så efterfrågas av kommunen. Dock uppges att detta sällan efterfrågas i praktiken. Vid tidpunkten för granskningen finns inte heller absoluta krav på att utveckling, testning och produktionssättning av ändring ska genomföras av olika personer i kontrollsyfte.

Att kommunen inte är formellt involverade i den fulla processen för förändringshantering, och att ansvar inte separeras för de olika aktiviteterna i genomförandet av en förändring mellan olika personer, medför risk att eventuella fel inte upptäcks och att felaktiga förändringar genomförs i kommunens verksamhetssystem. Detta kan påverka systemens prestanda negativt och leda till hinder i kommunens verksamhetsutövande, särskilt vad gäller kritiska system där tillgänglighet är av stor vikt.

Rekommendation

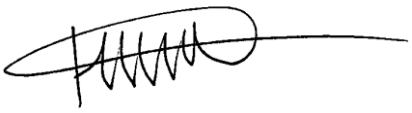
Kommunstyrelsen rekommenderas att:

1. Se till att kommunen ser över sin roll i processen för förändringshantering för de system som driftas hos SOLTAK. Förslagsvis bör kommunen säkerställa att processen för förändringshantering är utformad på ett för kommunen tillfredsställande sätt där ansvar för de olika aktiviteterna i genomförandet av en förändring separeras mellan olika personer i kontrollsyfte, samt att man är tillräckligt informerad i de olika besluten såsom beslut om acceptanstestning och produktionssättning, där detta bedöms nödvändigt.

Göteborg den 31 augusti

Rebecka Arén
Konsult
Ernst & Young AB

Rebecca Johansson
Konsult
Ernst & Young AB



Hardik Patel
Kvalitetsansvarig konsult (CISA)
Ernst & Young AB

Bilaga 1: Källförteckning

Intervjuade funktioner

- Digitaliseringschef Stenungsunds kommun
- Säkerhetssamordnare Stenungsunds kommun
- VD SOLTAK
- IT-chef SOLTAK
- IT-arkitekt SOLTAK
- Ekonomichef SOLTAK
- Chef Affärsstöd SOLTAK

Dokument från Stenungsunds kommun

- Aktieägaravtal SOLTAK AB
- Avtal mellan SOLTAK AB och Stenungsunds kommun..
- Bilaga 1 2017-09-26 RSA uthyrning behörighet serverhall
- Bilaga 2 Åtgärdsanalys
- Bolagsordning SOLTAK AB
- Hyresavtal om upplåtelse av serverhall
- Informationssäkerhetspolicy Stenungsunds kommun
- IT-säkerhetspolicy Stenungsunds kommun
- Leverantörsdialog mall
- Personuppgiftsbiträdesavtal mellan kommunstyrelsen nämnderna och SOLTAK
- Säkerhetsinstruktion drift
- Tjänstebeskrivning Datacenter
- Tjänstebeskrivning IT Arbetsplats
- Tjänstebeskrivning Nät
- Ägardirektiv SOLTAK AB

Dokument från SOLTAK

- Account master data
- Avtal om upplåtelse av serverhall i Stenungsund
- Backup och övervakning OS Ticket
- Beställning av behörighet för Självservice HR Lön
- Changeprocessen
- Design Backup Restore Soltak
- Integration design Personec-MIM-AD

- Incidentrapport Extern Mall
- Major Incident Manager SNABBGUIDE
- Rapport Backuper DPM
- Roller i Självservice HR Lön 200603
- Rutin - Administrera användare och behörigheter i Agresso
- SAMS Dokumentation
- SAMS Teknisk Dokumentation
- Soltak Backup Datacenter
- Soltak LE - DPM Documentation - 1.0
- Upplägg Ändring Avslut av användare i Agresso 2018-06-07
- Återläsning av enstaka filer från backup
- Återläsning av enstaka filer Shadowcopy
- Återläsning av server från Bare-Metal backup
- Återläsning av VHDX från backup
- Återläsning av VM från backup