Södertälje kommun

Revisorerna

Revisionsskrivelse

2020-05-14

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Revisionsrapport nr 2/2020 – Granskning av informationssäkerhet

På vårt uppdrag har EY genomfört en granskning av kommunens arbete med informationssäkerhet. Syftet har varit att bedöma om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med IT- och informationssäkerhet är ändamålsenligt.

Granskningen är också en uppföljning av den granskning vi gjorde 2017. De brister av allvarlig karaktär vi då uppmärksammade är i stort sett åtgärdade. Sedan dess har hotbilden inom IT och mot offentliga institutioner ökat, vilket ställer nya krav på IT-säkerheten.

Den aktuella granskningen visar att kommunens styrning av arbetet med IT- och informationssäkerhet har en generellt god mognadsnivå, men att det finns kvarvarande och nya brister som behöver åtgärdas.

Kommunstyrelsens kommentarer till rapporten och åtgärdsplan önskas senast den 31 augusti 2020.

För revisorerna i Södertälje kommun

Christer Björk

Elisabet Komheden

Bilaga: Revisionsrapport nr 2/2020– Granskning av informationssäkerhet

Revisionsrapport nr 2/2020

Södertälje kommun

Rapport: Informationssäkerhetsgranskning

April 2020

Magnus Andersson

Building a better working world

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Södertälje har EY genomfört en granskning av informationssäkerhet och datalagring vad gäller policyer, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå i kommunen. Syftet med granskningen har varit att undersöka på vilket sätt kommunen arbetar för att upprätta en god informationssäkerhet och en del av granskningen har varit att följa upp på de iakttagelser som noterades vid EYs granskning 2017. Granskningen har byggt på EYs ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor.

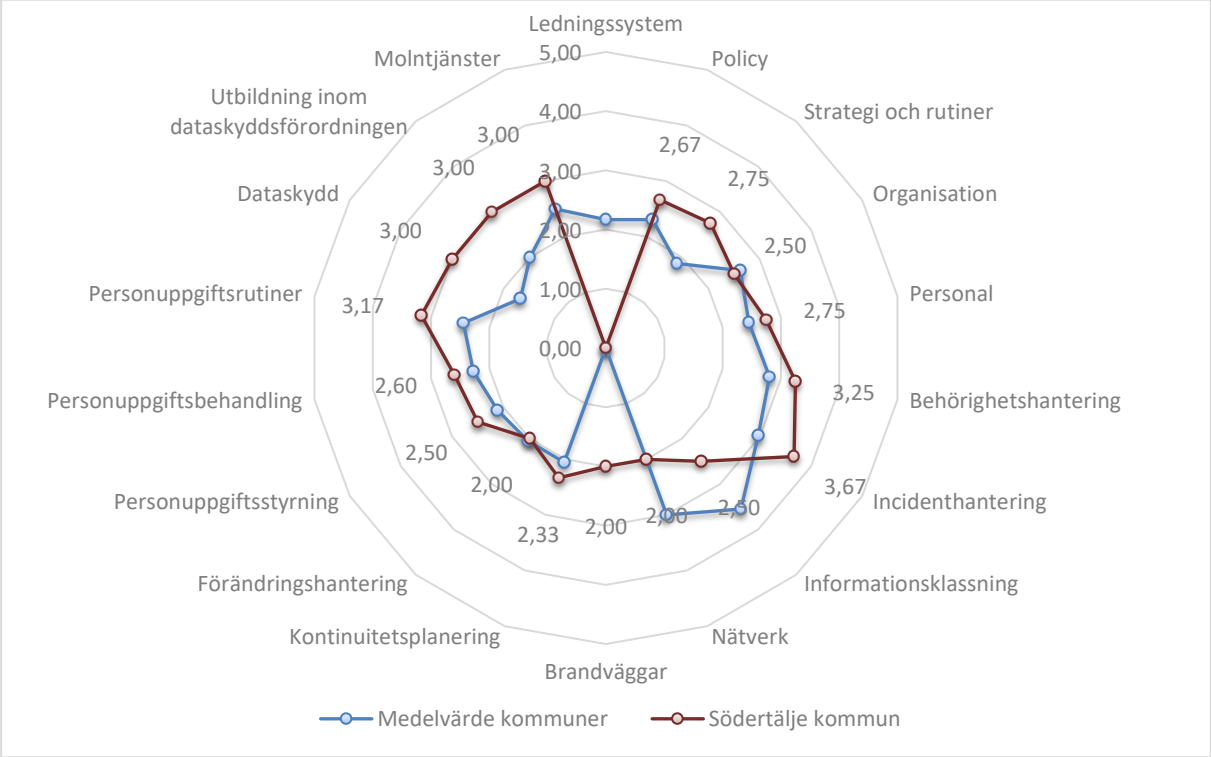
Övergripande slutsatser

Granskningen har noterat att kommunens styrning av arbetet med IT- och informationssäkerhet anses ha en generellt god mognadsnivå. Kommunens övergripande styrning fungerar väl där tydliga styrdokument med mål och riktlinjer gällande informationssäkerhet finns dokumenterade samt att roller och ansvar har definierats där ansvariga person har tillsatts för att hantera informationssäkerhet i de olika verksamheterna. Kommunen arbetar kontinuerligt med förbättringsarbete och har identifierat ett behov av att utöka kompetensen inom kommunen kopplat till informationssäkerhet. För att ytterligare förbättra arbetet med informationssäkerhet bör kommunen säkerställa att rätt prioriteringar görs i samband med budgetering för säkerhetsarbetet samt att regelbundet analysera kommunens kompetensbehov kopplat till informationssäkerhet.

Genomförd granskning av Södertälje kommun har även bedömt att det föreligger förbättringspotential kring uppföljning av beslut och styrdokument relaterat till informationssäkerhet. *Informationssäkerhetspolicyn* samt *riktlinjer för informationssäkerhet* är välskrivna dokument som kan användas som bas för informationssäkerhetsarbetet för samtliga verksamheter inom kommunen. Även inom arbetet kopplat till datalagring existerar det en klar förbättringspotential och då främst inom arbetet kopplat till informationsklassificering och en generell kontroll av de informationstillgångar som kommunen besitter.

Gällande uppföljningen av informationssäkerhetsgranskningen från 2017, anser EY att majoriteten av iakttagelser som noterades är åtgärdade. Endast iakttagelsen kring uppdatering av informationssäkerhetspolicyn ansågs ej vara helt åtgärdad då denna i nuläget är i en version från 2017. Detta är något som kommunen är medveten om och ett arbete kring att identifiera områden som behöver uppdateras skedde under 2019, men förändringarna implementerades aldrig. Sammantaget anses kommunen ha åtgärdat de iakttagelser som noterades under granskningen 2017 i hög utsträckning och i det fallet där iakttagelsen ej ansågs vara åtgärdad finns en god plan samt medvetande för hur detta ska åtgärdas framöver.

I figuren nedan ges ett överskådligt och sammanfattande resultat av Södertälje kommuns informationssäkerhetsarbete utifrån EYs ramverk för granskning av IT- och informationssäkerhet. Något som bör poängteras är att ett arbete kring implementering av Ledningssystem för Informationssäkerhet (LIS) är initierat och planerat inom kommunen, men i nuläget finns inget LIS implementerat och denna kategori har därför ej poängsatts. Det genomsnittliga resultatet har baserats på flertalet tidigare genomförda granskningar av kommunala verksamheter i Sverige. Ingen data fanns att tillgå för medelvärdet för kategorin "Brandväggar" och detta är anledningen till att medelvärdet för denna kategori ej är poängsatt.



Figur 1: Sammanfattande betyg av informationssäkerhetsarbete (skalan beskrivs mer utförligt under avsnittet 1.3 Metod och Genomförande)

Innehåll

1. Bakgrund

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

I sin årliga risk- och konsekvensanalys har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med informationssäkerhet samt IT-risker kopplat till verksamhetskritiska system inom kommunen. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med informationssäkerhet. Riskerna är inte specifikt relaterade till Södertälje kommun utan gäller hela den offentliga sektorn.

Under 2017 genomfördes en granskning av såväl informationssäkerhet som personuppgiftshantering på Södertälje kommun. Denna resulterade i ett flertal iakttagelser av kritisk karaktär. Sedan dess har den generella hotbilden både inom IT i allmänhet och mot offentliga institutioner i synnerhet ökat.

1.1 Syfte och revisionsfrågor

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. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. Denna granskning fungerar dels som en uppföljning på informationssäkerhetsgranskningen från 2017 och dels som en uppdaterad nulägesanalys. Följande revisionsfrågeställningar har använts för att konkretisera syftet:

- Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
- Är arbetet med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
- Kan kommunens arbete kopplat till datalagring bedömas som ändamålsenligt?
- I vilken utsträckning har kommunen åtgärdat identifierade iakttagelser från 2017, avseende IT-säkerhet?

1.2 Avgränsningar

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 informationssäkerhetsarbetet. Denna granskning omfattar vissa generella delar av personuppgiftshantering, men går inte in i detalj på efterlevnad av dataskyddsförordningen (GDPR).

1.3 Metod och genomförande

Granskningen har byggt på EYs 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 har insamlats både genom granskning av relevanta dokument, samt genom att EYs specialister genomför granskningsmöten med relevanta personer i kommunen.

Inledningsvis granskades relevant dokumentation kring kommunens rutiner och processer av EY. Parallellt hölls granskningsmöten med kommunens representanter för att gå igenom de områden som är inkluderade i EYs ramverk för granskning av IT- och informationssäkerhet i kommuner. Under granskningen har dock inga stickprovstester utförts, vilket innebär att efterlevnad av rutiner och kontroller ej har testats. Därefter analyserades och bedömdes den samlade bilden av dokumentation samt information inhämtad via granskningsmöten.

Under granskningen intervjuades:

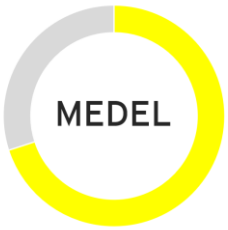
- Gunnar Hamber, Informationssäkerhetsansvarig
- Jonas Knutsson, IT-chef
- Fredrik Weller, IT-säkerhetsspecialist och IT-arkitekt

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

1.3.1 Bedömning avseende iakttagelser

Under granskningen har EY identifierat iakttagelser inom granskade områden. För varje iakttagelse har EY lämnat rekommendationer som syftar till att stödja Södertälje kommun i dess framtida arbete med informationssäkerhet. De av EY identifierade iakttagelserna har klassificerats enligt tre prioriteringsnivåer avseende hur omfattande dess eventuella inverkan anses vara:

Prioritering låg: Observation som ej direkt påverkar 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.



Prioritering medel: Observation som 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 hög: Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.

1.3.2 Bedömning avseende sammanfattande betyg av informationssäkerhetsarbete

Under granskningen har EY gjort en sammanfattande betygsättning på 18 områden på en skala 1-5. Skalans definition presenteras nedan:

1	Saknas helt / fungerar mycket bristfälligt utan rutiner
2	Existerar men har inte formellt definierats / fungerar bristfälligt utifrån begränsade rutiner
3	Har definierats med delvis efterlevnad / fungerar godtagbart utifrån definierade rutiner
4	Har definierats och förvaltas med god efterlevnad / fungerar väl utifrån definierade rutiner
5	Har definierats och förvaltas med mycket god efterlevnad / fungerar optimalt utifrån mycket väl definierade rutiner

2. Analys

I följande avsnitt redogörs först en nulägesanalys och beskrivning av Södertälje kommuns nuvarande arbete kopplat till informationssäkerhet. Utifrån detta följer en uppföljning och status av tidigare års iakttagelser samt de nya iakttagelser som identifierades under granskningen.

2.1 Nulägesanalys

2.1.1 Strategi, styrning och organisation

2.1.1.1 Styrdokument

Södertälje kommuns arbete med informationssäkerhet beskrivs på en övergripande nivå i den nuvarande informationssäkerhetspolicyn som fastslogs 2017. I *Informationssäkerhetspolicyn* fastställer kommunstyrelsen Södertälje kommuns syn på informationssäkerhet samt övergripande mål och intentioner. Detta fungerar således som det överordnade och styrande dokumentet och i dokumentet *Riktlinjer för informationssäkerhet* beskrivs vilka rutiner och säkerhetslösningar som måste etableras för att uppfylla de mål som beskrivs i *Informationssäkerhetspolicyn*. Riktlinjerna syftar till att etablera en gemensam säkerhetsnivå som kommunens olika delar minst förväntas uppfylla. Anställda kan nå dokumenten via intranätet.

Enligt Södertälje kommuns *Riktlinjer för informationssäkerhet* ska policyn revideras årligen och under en handlingsplan för informationssäkerhet under 2019 identifierades behov av justeringar, men dessa har ännu inte fastställts och initierats. Samtidigt har ett arbete kring att etablera ett Ledningssystem för informationssäkerhet (LIS) enligt ISO27000-standarden initierats under 2019.

2.1.1.2 Organisation och ansvarsfördelning

I nedanstående bild beskrivs Södertälje kommuns organisationsstruktur.

Figur 2: Organisationskarta - Södertälje kommun

Kommunfullmäktige beslutar om Södertälje kommuns allmänna mål, även när det gäller användning av IT, digitalisering och verksamhetsutveckling. Kommunstyrelsen beslutar sedan om det övergripande styrdokumentet *Informationssäkerhetspolicy* som styr kommunens arbete med informationssäkerhet. I policyn beskrivs följande ansvarsområden gällande informationssäkerhet:

- *Kommunstyrelsen* har det yttersta ansvaret för kommunens informationssäkerhetsarbete och fastställer detta genom kommunens informationssäkerhetspolicy.
- *Informationssäkerhetsansvarig* har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig har även som uppgift att samordna kommunens personuppgiftsombud.
- *Informationsägarna* har det övergripande ansvaret för den information som används inom en avgränsad verksamhet.
- *Systemägarna* har det övergripande ansvaret för respektive system och hur informationen hanteras i systemet.
- *Systemförvaltarna* ansvarar för information som lagras eller bearbetas i IT-system och kan ses som systemägarnas utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.
- *Chefer* ansvarar för att dess medarbetare är medvetna om och arbetar efter policyn.

2.1.1.3 Externa leverantörer och hantering av leverantörsavtal

Vid samtliga upphandlingar av informationssystem inom Södertälje kommun ställs upphandlingskrav som beskriver både funktionella krav och icke-funktionella krav och hur externa leverantörer skall hantera den information som finns inom respektive system. Dessa krav fastställs i avtalet för varje individuellt system och baseras bland annat på hur verksamhetskritiskt systemet är och vilken typ av känslig data som systemet hanterar. Som stöd för denna analys används SKR:s klassificeringsverktyg KLASSA. Beroende på upphandling kan berörd verksamhet antingen ta hjälp av centrala funktioner för hantering av kravställning eller i vissa fall hantera detta själva.

Systemägaren för respektive system ansvarar för att följa upp att relevanta avtal (SLA) finns med leverantörer och att dessa efterlevs. Informationsägaren för respektive system ansvarar sedan för att följa upp att SLA för systemet är i relation till informationsklassificeringen och hur kritiskt systemet är för verksamheten. Hur ofta denna uppföljning ska ske och mer specifika centrala riktlinjer för uppföljning av befintliga leverantörer och upphandlade system finns ej definierade.

2.1.1.4 Personal och utbildning

Det existerar i dagsläget ett behov av att utöka antalet medarbetare som arbetar med informationssäkerhet då det finns vakanser på ett antal positioner inom säkerhetsavdelningen. Detta till följd av att personal har gått i pension eller slutat och att dessa positioner ej har blivit ersatta samt att man inom kommunen har identifierat ett

behov av att utöka arbetet kring informationssäkerhet och således behöver rekrytera rätt kompetens för detta. Anledningen till att detta rekryteringsarbete och säkerställande av kompetens ej har genomförts kan dels bero på en budget- och prioriteringsfråga, dels på att det är problematiskt att hitta rätt kompetens och personal. Arbetet har dock påbörjats och i början av 2020 anställdes en ny chef för säkerhetsavdelningen och i samband med detta gjordes även en kartläggning över vilka kompetenser som behöver rekryteras framöver.

En utbildningsplan för dataskydd inom kommunen, dataskydd 2019, med målsättningen att i klarspråk kommunicera rutiner, öka medvetenhet om risker och sprida kunskap om kommunens incidenthantering påbörjades 2019. Utbildningsplanen syftar till att bidra med en generell kunskapshöjning inom dataskydd och incidenthantering för samtliga anställda. Strategin för detta är att nå ut med e-learnings till samtliga anställda och sedan ha specifika kurser för medarbetare som behöver fördjupa sin kunskap inom området, exempelvis dataskyddssamordnare. Från hösten 2019 ansvarar dataskyddsombud (DSO) för fortlöpande utbildning inom integritet och dataskydd.

Södertälje kommun och kommunkoncernen Telge AB har även identifierat ett behov av att genomföra ytterligare breddutbildningar inom informationssäkerhet. Ett arbete för att bygga upp en generell e-learningsplattform som kan användas är initierad och nästa steg är att fatta beslut om hur denna plattform ska användas för utbildningar inom informationssäkerhet. Som alternativ finns det möjlighet att nyttja en kurs "Informationssäkerhet i praktiken" finansierad av MSB i samverkan med SKR. Kommunen tittar även på en utbildningsform för att öka medarbetares kunskap inom området genom så kallade nano-learnings, vilket består av kortare och mer frekventa webb-kurser.

2.1.1.5 Styrning av åtkomsthantering

Det finns definierade processer för behörighetshantering som är beskrivna i *Riktlinjer för informationssäkerhet*. I detta dokument beskrivs processen på en övergripande nivå och anpassas sedan för varje nämnd och för varje system. På en central nivå har arbete kring att implementera rollbaserad behörighetsstyrning initierats, då detta anses skapa en mer lätthanterlig och säkrare process för att styra behörighetshantering. På en infrastrukturell nivå används även tilldelning av behörigheter via Active Directory (AD) i så stor utsträckning som möjligt och för de system som är verksamhetskritiska utförs periodisk genomgång av användare. För de verksamhetskritiska systemen används även tvåfaktorsautentisering för att skydda system från att ge olämpliga användare åtkomst.

2.1.2 Operationella rutiner

2.1.2.1 Användarinstruktioner

Södertälje kommun har definierat en övergripande anvisning för användningen av kommunens IT-miljö som gäller för alla användare i kommunens olika verksamheter. I denna övergripande anvisning beskrivs regler och riktlinjer för hur medarbetare ska använda kommunens datorer och andra digitala enheter, internet, e-post, lösenord och behörigheter.

2.1.2.2 Incidenthantering

Hantering av informationssäkerhetsincidenter beskrivs i *Riktlinjer för informationssäkerhet*. I de inköpta informationssystemen ansvarar leverantören för övervakning och kontroll av den tekniska driftmiljön och loggar incidenter orsakade av tekniska brister och externa störningar. Kritiska incidenter eskaleras omgående till beställaren (IT-avdelningen) och vid kvartalsvisa uppföljningar (säkerhetsforum) redovisar leverantören alla inträffade incidenter, typer och statistik samt analyser av sårbarheter.

Anställda, uppdragstagare och tredjepartsanvändare av informationssystem och tjänster har som ansvar att notera och rapportera alla observerade eller misstänkte säkerhetsbrister i system eller tjänster. Incidenter och säkerhetsmässiga svagheter ska rapporteras snarast till systemägare och informationssäkerhetsansvarig och servicedesk fungerar som en kontaktyta som samtliga anställda kan använda för att göra felanmälningar och rapportera incidenter. Servicedesk fungerar således som en "single-point-of-contact" för att kunna fånga upp händelser i verksamheten och logga tekniska och verksamhetsmässiga störningar.

Incidenter kopplade till personuppgifter hanteras av kommunens dataskyddsombud (DSO) och utsedda dataskyddssamordnare (DSS) som finns för varje nämnd. Dessa besitter störst kompetens kring personuppgiftshantering inom kommunen och har det yttersta ansvaret för att hantera incidenter kopplade till detta.

2.1.2.3 Programförändringsrutiner

Processer för hantering av förändringar i IT-system finns fastställda och dessa ska även följas för förändringar som är av system-infrastrukturell karaktär. Enligt denna process ska beslut kring programförändringar följa en CAB-process (Change Advisory Board) och samtliga förändringar ska kunna härledas till ansvarig beställare. Något som kan noteras är att utöver den centrala IT-funktionen i Södertälje kommun har nämnder eller koncernbolag egna IT-samordnare där denna process kan se annorlunda ut.

2.1.2.4 Driftdokumentation och kontinuitetsplanering

Kommunen har en centralt utarbetad och fastställd krisplan som formaliserar arbetet med kris och verksamhetskontinuitet. Respektive nämnd och kontor med kritisk verksamhet har även verksamhetskontinuitetsplaner som avser den egna förmågan att upprätthålla sin egen verksamhet. Enligt *Riktlinjer för informationssäkerhet* ska det inom respektive verksamhet och nämnd utarbetas planer för att upprätthålla eller återställa drift och säkerställa tillgänglighet till information efter avbrott eller fel i kritiska processer. Det är respektive systems systemägare som är ansvarig för att hålla systemets kontinuitetsplan aktuell för att säkerställa att verksamheten kan drivas även vid inträffandet av en kris eller katastrof.

När det kommer till systeminfrastrukturell hantering av drift existerar riktlinjer för hur nätverk ska segregeras ur ett säkerhetsperspektiv, hur brandväggar ska upprätthållas

samt hantering av backups. Driften av brandväggar är något som sköts av en extern leverantör.

2.1.3 Dataskydd och datalagring

2.1.3.1 Personuppgiftshantering

För att säkerställa att efterlevnad kring dataskyddsförordningen (GDPR) upprätthålls följer Södertälje kommun dataskyddsförordningens artikel 35 gällande konsekvensbedömning avseende dataskydd. Kommunen använder en metod för tröskelanalys för konsekvensbedömning, på engelska benämnd Data Protection Impact Assessment (DPIA). Kommunens dataskyddsombud (DSO) har ansvar för att säkerställa att respektive nämnds område behandlar personuppgifter på ett korrekt och lagligt sätt och är även den part som rapporterar till Datainspektionen. Inom varje nämnd finns även dataskyddssamordnare (DSS) som hanterar och samordnar dataskyddsfrågor lokalt och gentemot kommunens dataskyddsombud. Utöver detta har även ett strategiforum för dataskydd etablerats som ansvarar för samordning för hantering av personuppgifter inom kommunen. Tillsammans med detta strategiforum har även en årsplan för dataskyddsarbete 2020 presenterats och består av följande aktiviteter:

- Information från DSO per förvaltning till nämnderna
- Utbildning
- Informationsmaterial
- Registerhållning
- DPIA
- Samverkan med digitalisering
- Incidenthantering (generellt: GDPR, säkerhet och informationssäkerhet)
- Registerförfrågningar
- Gemensamma dokument och riktlinjer

Personuppgiftsincidenter hanteras utefter samma process som den vanliga incidenthanteringen. Alla personuppgiftsincidenter ska rapporteras till servicedesk så fort som möjligt efter att incidenten har upptäckts. Detta gäller även om incidenten hunnit bli åtgärdad. När en rapport anmälts följer en process för bedömning, dokumentation och rapportering av personuppgiftsincidenter. Om en personuppgiftsincident innebär en risk för registrerades rättigheter gäller en tidsgräns 72 timmar från kännedom för kommunen för att rapportera till Datainspektionen. Via en länk till en uppsatt e-tjänst kan personuppgiftsincidenter rapporteras.

Kommunen tillhandahåller ett register över den data kopplat till personuppgifter som hanteras av kommunen. Detta register avser att uppfylla artikel 30 i dataskyddsförordningen (GDPR) och beskriver exempelvis vilka kategorier av personliga data som kommunen hanterar. För hantering av dessa används verktyget OneTrust där uppgifter som namn på behandlingen, organisation och informationsägare är förtecknat. För tillfället finns 484 aktiva behandlingar. För behandlingar som utförs av andra parter är personuppgiftsbiträdes-avtal (PUB-avtal) tecknat med dessa leverantörer. Efterlevnadskontroll av leverantör skall genomföras (nästa gång under hösten 2020) av anlitade leverantörer där ett PUB-avtal upprättats. I PUB-avtalen fastställs en revisionsrätt

hos leverantörer. Kontrollerna ska säkerställa att Södertälje kommuns informationstillgångar samt de registrerades personuppgifter hanteras på ett korrekt och säkert sätt. Urvalet av leverantörer som kontrolleras baseras på en riskbedömning som prioriterar de leverantörer som har högst risk.

Kommunen följer dataskyddsförordningens krav på laglig grund för behandling av persondata, och för de behandlingar där samtycke efterfrågas följer kommunen artikel 6, där inhämtning, förteckning över samtycke och återtagande av samtycke beskrivs. Rutiner för de situationer där det krävs samtycke finns dokumenterat och tillgängligt för all personal via Södertälje kommuns intranät.

Kommunen har definierat rutiner för gallring och lagring av personuppgifter. Dessa hanteras enligt dokumenthanteringsplaner, som är styrande dokument för alla offentliga verksamheter. Dokumenthanteringsplanen redovisar vilka allmänna handlingar som finns vid en myndighet, och anger vilka handlingar som kan gallras och vilka som ska bevaras. I Södertälje kommun är kommunstyrelsen arkivmyndighet och stadsarkivet är det beredande och verkställande organet. Varje nämnd inom kommunen har, i samråd med stadsarkivarien, upprättat och beslutat om sin dokumenthanteringsplan. Samtliga dokumenthanteringsplaner är publicerade på kommunens intranät

2.1.3.2 Informationsklassning och datahantering

Södertälje kommun använder SKR:s klassificeringsverktyg KLASSA för att informationsklassificera sina informationssystem. Syftet med informationsklassningen är att rätt åtgärder ska väljas för att skydda information i respektive system samt för att få en förståelse över vilka system som anses som mest verksamhetskritiska. Systemägaren för respektive system ansvarar för att informationsklassningen sker. Under utförda intervjuer under granskningen har det lyfts att 108 av kommunens 340 informationssystem är i behov av klassning eller uppdatering och detta är en del av ett kontinuerligt IT-samordningsprogram. Vidare har det noterats att det inte finns någon övergripande kontroll eller process på plats för att enkelt följa upp vilka system som inte har använt sig av KLASSA.

Informationsklassningen noteras i förteckningen över applikationer och system men själva klassningen sker i verktyget KLASSA (enligt riktlinjer för informationssäkerhet). I aktuell förteckning över applikationer och system har bedömningen gjorts att cirka 80 hanterar personuppgifter varav cirka 12 bedöms hantera personuppgifter som anses extra känsliga. Affärskritikalitet är angivet för de applikationer/system där det varit relevant att göra en bedömning och för dessa applikationer/system har följande klassning gjorts:

- hög: 55,
- medel: 20,
- låg: 56.

2.1.3.3 Molntjänster och datalagring

Ett stort antal av kommunens IT-system och applikationer är utlagda på tredjeparter och kommunen har i nuläget 87 leverantörer, där sju leverantörer tillhandahåller system för

fler än 1000 användare. Tjänsteleverantören Tieto är ett exempel på en särskild viktig samarbetspartner och hanterar driften för flertalet verksamhetskritiska system, exempelvis system inom vård- och omsorg och skolsystem. De vanligaste leveransmodellerna för IT-system inom kommunen är klientinstallation (77), Software as a Service (SaaS) (34), tjänsteleverans /applikationsdrift från Tieto (9) samt Platform as a Service (PaaS) från Tieto (4). Leverantörsavtal ses över kontinuerligt och avtalstider dokumenteras. Mer om hur leverantörsavtal hanteras beskrivs i 2.1.1.3 Externa leverantörer och hantering av leverantörsavtal.

För personuppgifter hanterade i molntjänster så följer kommunen SKR:s vägledning och riktlinjer. Dessa riktlinjer är framtagna av SKR för att vägleda och hjälpa kommuner och regioner att analysera frågor om juridik och säkerhet för molntjänster. Dessa riktlinjer belyser bland annat vikten av att rättsliga förutsättningar och säkerhet för information analyseras innan implementering av molntjänster. I de fall där riktlinjerna är tvetydiga eller svårtolkade har kommunen som princip att avstå från att använda sig av molntjänster.

2.2 Uppföljning av tidigare års iakttagelser

Vid den tidigare genomförda granskningen av Södertälje kommuns informationssäkerhet 2017, noterades ett antal iakttagelser samt risker kopplade till dessa. En del av denna granskning har således varit att följa upp dessa iakttagelser och bedöma nuvarande status och huruvida åtgärder har tagits eller initierats. Granskningen har huvudsakligen fokuserat på de mest kritiska iakttagelser som har markerats som ”hög risk”.

ID	Granskningsområde	Iakttagelse 2017	Status 2020	Bedömning 2020
2017.1	IT-leverantörer	**Kommunen förlitar sig på leverantörerna gällande säkerheten av systemen utan att kontrakt följs upp eller granskas.** Kommunen genomför exempelvis inte några penetrationstester utan förlitar sig på att leverantörerna och att verksamheterna själva uppfyller säkerhetskraven. Identifiering av tekniska sårbarheter som kan vara blottade för en eventuell angripare säkerställs således enbart genom avtal med leverantörerna, vilka i de flesta fall inte följs upp.	Systemägaren för respektive system ansvarar för att följa upp avtal med leverantörer. I dessa avtal ska det förtydligas att utveckling sker enligt bestämda krav. Enligt ”Riktlinjer för Informationssäkerhet” ska system som har förändrats innan produktionssättning genomgå en testprocess som består av enhets-, system-, integrations- och acceptanstester. Dessa ska genomföras av den person eller enhet som har beställt förändringen. Utöver detta så har kommunen infört följande åtgärder: - Kontaktperson från leverantören för den samlade leveransen utsedd - En rapportstruktur för kontroll och uppföljning är införd - Avtalsuppföljning för leverans sker regelbundet - Ett fora för säkerhet (Säkerhetsrådet) etablerad för övervakning och kontroll av IT-	Åtgärdad.

ID	Granskningsområde	Iakttagelse 2017	Status 2020	Bedömning 2020
			säkerhet, incidenthantering och sårbarheter - Specifik informationsklassning för samtliga kontrakterade system/tjänster initierad	
2017.2	Policyer och styrdokument	**Kommunen har inte uppdaterat sin informationssäkerhetspolicy** Policyn författades för ca 3 år sedan och har inte uppdaterats sedan dess.	Den nuvarande versionen av informationssäkerhetspolicyn uppdaterades 2017, och den har således uppdaterats sedan den genomförda granskningen 2017 då iakttagelsen först noterades. Men policyn har fortfarande inte uppdaterats lika frekvent som det är uttalat. I Informationssäkerhetspolicyn noteras det att uppföljning och revidering av policyn ska ske regelbundet och det finns en uttalad ambition om att årligen gå igenom och uppdatera policyn. Ett arbete kring att identifiera områden som behöver uppdateras skedde under 2019, men förändringarna implementerades aldrig.	Ej åtgärdad.
2017.3	Information och utbildning	**Kommunen genomför inga utbildningsinsatser inom informationssäkerhet** Det saknas ett strukturerat utbildningsprogram inom organisationen för att säkerställa adekvat kunskapsnivå inom informationssäkerhet.	En Utbildningsplan för breddutbildning ”Dataskydd 2019” har antagits vilken förväntas bidra med en generell kunskapshöjning inom informationssäkerhet. En breddutbildning med samtliga anställda som målgrupp har genomförts, kompletterad med lärarledd fördjupning för dataskyddssamordnare. Från hösten 2019 ansvarar dataskyddsombud (DSO) för fortlöpande utbildning inom integritet och dataskydd. Kommunen och Telge AB har även identifierat ett behov av att genomföra breddutbildningar inom informationssäkerhet. Ett arbete för att bygga upp en generell e-learningsplattform som kan användas är initierad. Även styrning av medarbetare genom nanolearning prövas.	Åtgärdad.
2017.4	Risker kopplade till informationssäkerhet	**Gällande informationssäkerhet saknar kommunen en konkret incidentshanteringsplan** Kommunens processer och rutiner för säkerhetsriskhantering och incidenthantering är decentraliserade och styrs av skilda kontor.	En process för att hantera säkerhetsincidenter finns inom kommunen. IT-säkerhetsrelaterade incidenter anmäls och hanteras av servicedesk centralt. Övervakning och incidenthantering i driftmiljön hanteras av driftleverantören.	Åtgärdad.

ID	Granskningsområde	Iakttagelse 2017	Status 2020	Bedömning 2020
			Dataskyddsombud är utsedda för samtliga förvaltningar och fungerar som mottagare av incidenter kopplade till personuppgifter och informationssäkerhet.	
2017.5	GDPR	**Kommunens förberedelse inför GDPR 2018 har påbörjats och bedöms generellt vara i startgropen.** Utbildning och möten med chefer har påbörjats. Dock inväntar många ett centralt initiativ varpå arbetet med GDPR i många verksamheter står still. Arbete med GAP-analys och efterföljande åtgärdsplaner för att säkerställa regelefterlevnad avseende alla delar av dataskyddsförordningen avses påbörjas enligt information.	Projektet kring GDPR är genomfört och resultatet överlämnat till förvaltning sommaren 2019. Riktlinjer har även satts upp för det kontinuerliga arbetet med GDPR inom organisationen och dataskyddsombud med ansvar för personuppgiftshantering har valts ut för respektive nämnd.	Åtgärdad.

2.3 Nya iakttagelser och kvarstående iakttagelser

2.3.1 Kommunen har ej tillräckligt med resurser inom arbetet kring informationssäkerhet

Iakttagelse 	Det finns vakanser inom flertalet positioner kopplade till säkerhetsarbetet och man har inom kommunen identifierat ett behov av att utöka de resurser som arbetar med samt kompetensen kopplat till arbetet med informationssäkerhet.
Risk	Utan rätt bemanning kommer arbetet kring informationssäkerhet bli lidande och kan potentiellt leda till att väsentliga och viktiga aktivitet bli bort prioriterade.
Rekommendation 	Södertälje kommun rekommenderas att: ▸ Säkerställa att rätt prioriteringar görs i samband med budgetering för säkerhetsarbetet. ▸ Regelbundet analyserar kommunens kompetensbehov kopplat till informationssäkerhet.

2.3.2 Den nuvarande informationsklassningen är ej i linje med den fastställda

policyn.

Iakttagelse 	Kommunen använder SKR:s klassificeringsverktyg KLASSA för att informationsklassificera sina informationssystem, men 108 av 340 system är i behov av klassning eller av en uppdatering av klassning.
Risk	Avsaknaden av en informationsklassning ökar risken för att informationssäkerhetsrelaterade risker inte upptäcks. Att inte samtliga av kommunens system informationsklassas i enlighet med beslutad policy ökar risken för att organisationen ska vara inkapabel att upptäcka och hantera informationssäkerhetsrelaterade incidenter i tid och på ett effektivt sätt.
Rekommendation 	Samtliga systemägare bör uppdateras gällande kravet kring att informationsklassning ska utföras i det gemensamma verksamhetssystemet KLASSA. Kommunen rekommenderas att följa upp och säkerhetsställa att alla informationstillgångar analyseras och bedöms i KLASSA.

2.3.3 Ägandeskap av informationssäkerhetspolicyn och säkerställande att den uppdateras är ej tydligt

Iakttagelse 	Det finns ambition om en årlig genomgång av policyn, men varken "Informationssäkerhetspolicy" eller "Riktlinjer för informationssäkerhet" har uppdaterats sedan 2017. Detta noterades även som en observation under granskningen 2017.
Risk	I och med en snabb IT-utveckling finns risk att policyn och åtgärder inte täcker viktiga områden eller är anpassad till organisations och omvärldens förändrade omständigheter.
Rekommendation 	Det rekommenderas att uppdatera policyn kontinuerligt så att den reflekterarar organisations nuvarande behov samt omvärldens möjligheter och krav. Eftersom det är kommunstyrelsen som måste godkänna policyn föreslås att det årligen finns en agendapunkt som behandlar eventuella tillägg och förändringar till policyn.

2.3.4 Uppföljning kring huruvida centrala riktlinjer kring informationssäkerhet efterlevs saknas för vissa verksamheter

Iakttagelse 	IT-initiativ inom olika nämnder och koncernbolag styrs till viss del decentraliserat och till följd av detta saknas central uppföljning kring huruvida somliga verksamheter inom kommunen faktiskt lever upp till de centrala riktlinjerna kring informationssäkerhet som finns inom kommunen.
Risk	Utan kontinuerlig uppföljning finns det risk att varje enskild verksamhet inom kommunen missar väsentliga delar som har beslutats i de centrala riktlinjerna för informationssäkerhet.
Rekommendation 	Kommunens övergripande informationssäkerhetsansvarig rekommenderas att: 1. Definiera nyckeltal som samtliga verksamheter måste efterleva, exempelvis följa upp på vilka verksamheter som inte har fullgjort informationssäkerhetsklassning av sina verksamhetssystem. 2. Skapa en rutin för att periodvis följa upp definierade nyckeltal och på så vis säkerställa att kommunen arbetar med informationssäkerhet på ett enat sätt genom alla verksamheter.

2.3.5 Centrala riktlinjer för användandet av informationsbehandlingstjänster av utomstående organisationer och leverantörer saknas

Iakttagelse 	Systemägaren ansvarar för att följa upp att relevanta avtal (SLA) som finns med leverantörer. Informationsägaren ansvarar för att följa upp att SLA för system som hanterar informationen är i relation till informationsklassning och hur kritiskt systemet är för verksamheten. Det saknas dock helhetsriktlinjer eller centralt stöd för samtliga systemägare och informationsägare för hur denna process ska gå till.
Risk	Risk att leverantörer inte levererar en tjänst i enlighet med överenskommet avtal. Vidare finns en risk för minskad kontroll kring krav på leverantörs arbete rörande informationssäkerhet.
Rekommendation 	Inför en sammanhållen riskfunktion inom kommunen som ett stöd till de enskilda förvaltningarna för att hantera och följa upp utomstående organisationer och leverantörer. Tydliggör rapporteringsvägar, innehåll i rapportering (med koppling mot mål/KPI:er, förslag till aktiviteter och budget) och ansvar/befogenheter för hantering av informationssäkerhetsrisker.

2.3.6 Det saknas uppföljning av att risk- eller sårbarhetsanalys har genomförts i samband med informationsklassningen av kommunens informationssystem

Iakttagelse 	Kommunen förlitar sig på SKR:s verktyg KLASSA för informationsklassning och i vissa fall genomförs ingen kompletterande risk- eller sårbarhetsanalys som komplement till verktyget. Det saknas central uppföljning kring vilken utsträckning som risk- eller sårbarhetsanalyser har genomförts.
Risk	Avsaknaden av en formaliserad process för uppföljning av riskanalys och åtgärdsplan ökar risken för att organisationen ska vara dåligt utrustad att upptäcka och hantera informationssäkerhetsrelaterade incidenter i tid och på ett effektivt sätt.
Rekommendation 	Södertälje kommun rekommenderas att införa en uppföljning kring vilken utsträckning som risk-och sårbarhetsanalyser har genomförts. Södertälje kommun rekommenderas även för de mest känsliga och kritiska informationssystemen (gällande konfidentialitet, riktighet och tillgänglighet) utföra djupare risk- och sårbarhetsanalyser. MSB tillhandahåller stöd i form av metoder som ger vägledning och tips som kan underlätta arbetet med en risk- och sårbarhetsanalys.

3. Slutsats

Granskningen har syftat till att på uppdrag av kommunens revisorer genomföra en övergripande genomgång av kommunens informationssäkerhetsarbete. Granskningen har utgått från fyra revisionsfrågor, vilka besvaras nedan.

Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?

Kommunens styrning av arbetet med IT- och informationssäkerhet anses ha en generellt god mognadsnivå. Kommunens övergripande styrning fungerar väl där tydliga styrdokument med mål och riktlinjer gällande informationssäkerhet finns dokumenterade samt att roller och ansvar har definierats där ansvariga person har utsatts för att hantera informationssäkerhet i de olika verksamheterna. Kommunen arbetar kontinuerligt med förbättringsarbete och har identifierat ett behov av att utöka kompetensen inom kommunen kopplat till informationssäkerhet. Det finns i nuläget flertalet vakanser inom positioner kopplat till säkerhetsarbetet och en anledning till detta kan vara kopplat till budget samt prioriteringar inom kommunen. För att ta arbetet med informationssäkerhet till nästa nivå bör kommunen säkerställa att rätt prioriteringar görs i samband med budgetering för säkerhetsarbetet samt att regelbundet analysera kommunens kompetensbehov kopplat till informationssäkerhet.

Är arbetet med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?

Genomförd granskning av Södertälje kommun har bedömt att det existerar förbättringspotential kring uppföljning av beslut och styrdokument relaterat till informationssäkerhet. *Informationssäkerhetspolicyn* samt *riktlinjer för informationssäkerhet* är välskrivna dokument som kan användas som bas för informationssäkerhetsarbetet för samtliga verksamheter inom kommunen. Dessa dokument borde dock ses över mer kontinuerligt för att upprätthåll relevans och därför bör processen kring uppföljning ses över.

Det saknas även till viss del en strukturerad och kontinuerlig uppföljning och kontroll av arbetet kopplat till informationssäkerhet i syfte att säkerställa efterlevnad runt om i kommunens olika verksamheter. Ett sätt att utöka detta och ta arbetet kring informationssäkerhet till nästa nivå i kommunen kan vara att införa tydliga mätvärden eller nyckeltal för informationssäkerhet samt en periodisk rapportering av dessa för de olika nämnderna.

Kan kommunens arbete kopplat till datalagring bedömas som ändamålsenligt?

Gällande kommunens arbete kopplat till datalagring har granskningen visat att det existerar ett pågående arbete kring personuppgiftshantering med en hög medvetenhet inom kommunen. Kommunen har även tagit ett konservativt tillvägagångssätt för

införande av molntjänster och följer SKR:s riktlinjer. En del av arbetet kopplat till datalagring rör kommunens informationsklassning av olika informationstillgångar som återfinns i delar av verksamheten. I nuläget saknar 108 av 340 system informationsklassning via verktyget KLASSA. Ett viktigt komplement till informationsklassningen via verktyget är även att utföra en risk- och sårbarhetsanalys av de mest kritiska informationssystemen. Utifrån detta kan kommunen skapa en bättre överblick och förståelse över de mest kritiska informationstillgångarna och på ett mer proaktivt sätt implementera säkerhetsåtgärder för att skydda dessa. För att kunna använda ett riskbaserat tillvägagångsätt och kunna skydda de informationstillgångar som är mest kritiska för kommunen, är en essentiell del att ha förståelse och kontroll över vilka informationstillgångar som finns inom kommunen samt vilka system som hanterar dessa tillgångar och hur roller och ansvar hanteras för respektive tillgång.

I vilken utsträckning har kommunen åtgärdat identifierade iakttagelser från 2017, avseende IT-säkerhet?

Gällande uppföljningen av informationssäkerhetsgranskningen från 2017, anser EY att majoriteten av iakttagelser som noterades är åtgärdade. Endast iakttagelsen kring uppdatering av informationssäkerhetspolicyn ansågs ej vara helt åtgärdad då denna i nuläget är i en version från 2017. Detta är något som kommunen är medveten om och ett arbete kring att identifiera områden som behöver uppdateras skedde under 2019, men förändringarna implementerades aldrig. Samtidigt har ett initialt planeringsarbete kring att införa ett Ledningssystem för informationssäkerhet (LIS) enligt ISO27000-standard påbörjats och som då kommer ersätta den nuvarande informationssäkerhetspolicyn samt dess riktlinjer. Sammantaget anses kommunen ha åtgärdat de iakttagelser som noterades under granskningen 2017 i hög utsträckning och i det fallet där iakttagelsen ej ansågs vara åtgärdad finns en god plan samt medvetande för hur detta ska åtgärdas framöver.

4. Bilagor

4.1 Dokumentförteckning

4.1.1 Kommungemensamma dokument

- Användarförsäkran (2016)
- Roller och ansvar for IT och digitalisering i Södertälje kommun (2016)
- Informationssäkerhetspolicy (2017)
- Riktlinjer för informationssäkerhet (2017)
- Organisationsschema (2019)
- Rutin: Rapportering av personuppgiftsincidenter (2018)
- Rapport: Konsekvensbedömningar (DPIA) (2018)
- Krisplan 2015-2018
- Södertälje kommuns digitaliseringsstrategi (2019)

4.2 Definitioner

Active Directory (AD): Katalogtjänst vilken lagrar information om resurser (såsom användare). Separata IT-system kan kopplas till Active Directory och både inloggning och behörighetsroller i systemen kan således styras genom inställningar och rolluppsättning i Active Directory. Detta möjliggör för central användarhantering och automatisk inloggning.
Backup: Säkerhetskopia av den information som finns i en databas eller på en server.
Återläsningstest: För att säkerställa att en säkerhetskopia fungerar som den ska och inte är sönder eller ofullständig så är det god praxis att genomföra tester av de säkerhetskopior som genomförts. Testet går ut på att återläsa in kopian in på servern eller databasen igen och granska innehållets korrekthet och fullständighet.
Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.
Systemansvarig: Ansvarar för handhavandet och administrationen kopplade till systemet.
Systemägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.
Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.
Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.
Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och konfidentialitet. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.
Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.
Avbrottsplan: Dokumentation av de återstarts- och reservrutiner för datadriften som ska vidtas inom ramen för ordinarie drift för att informationssystemen ska kunna återstartas inom fastställd tid.
Penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.
SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats.
CAB (Change Advisory Board): Styrgrupp för att fatta beslut kring hantering av programförändringar och utveckling av verksamhetens informationssystem.
Dataskyddsombud (DSO): Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen, genom att till exempel utföra kontroller och utbildningsinsatser.
E-learningplattform: En plattform för att distribuera utbildningsmaterial till medarbetare och plattformen organiserar vanligtvis även kommunikation, innehåll, uppgifter och utvärdering.
Nano-learning: Korta återkommande utbildningar som erbjuds för anställda.

SaaS: Software as a service, är en typ av molntjänst som tillhandahåller programvara över internet. Applikationerna tillhandahålls i "molnet" och kan användas för en rad olika uppgifter för både privatperson och organisationer.
PaaS: Platform as a service, är en typ av molntjänst som tillhandahåller en datorplattform och en uppsättning programvarusystem som en service.

4.3 Förteckning över intervjuade funktioner

- Gunnar Hamber, Informationssäkerhetsansvarig
- Jonas Knutsson, IT-chef
- Fredrik Weller, IT-säkerhetsspecialist och IT-arkitekt