Södertälje kommun

KS20180202

SÖDERTÄLJE KOMMUN
Kommunstyrelsen
2018 -01- 23
Dnr | Rnr

2018-01-19
Tjänsteskrivelse

Kontor
Kommunstyrelsens kontor

Handläggare
Per Tegel
08-523 03131
Per.tegel@sodertalje.se

Kommunstyrelsen

Revisionsrapport nr 5/2017 – Granskning av informationssäkerhet

Dnr KS 17/376

Sammanfattning av ärendet

EY har under hösten 2017, på uppdrag av Södertälje kommuns revisorer, genomfört en granskning i syfte att undersöka på vilket sätt kommunen arbetar för att upprätta och upprätthålla en god informationssäkerhet. Under granskningen har ett antal kontroller och intervjuer med olika befattningshavare genomförts. Av granskningsrapporten framgår det att de mest väsentliga riskerna bedöms vara kopplade till fem huvudsakliga områden. Nedan redovisas och kommenteras dessa:

- *Kommunen har betydande delar av sin IT-verksamhet utkontrakterad till externa leverantörer. Det genomförs inga egen initierade säkerhetskontroller utan verksamheterna förlitar sig på att leverantörerna lever upp till de krav som är avtalade.*

  Kontroller genomförs till viss del sedan tidigare. Den egna kontrollverksamheten ökas kontinuerligt av teknik (utrustning, programvara mm), organisation, processer och individer. Prioriteringen av kontroller baseras på hur information är klassad i verksamhetssystemen.

- *Granskningen visar att kommunens informationssäkerhetspolicy inte har uppdaterats på tre år, vilket innebär en risk för att den inte är anpassad efter förändrade omständigheter i organisationen och i omvärlden.*

  Detta påstående är inte korrekt. Kommunstyrelsen antog en uppdaterad version av aktuell policy den 29 september 2017. Det är dock rimligt att anta den behöver ses över och eventuellt uppdateras årligen eller vid förändrade förutsättningar.

- *Det genomförs inga utbildningsinsatser i förvaltningen inom området informationssäkerhet.*

  Specifika informationssäkerhetsutbildningar kommer ske med början våren 2018, för både nyanställda och befintlig personal

- *Det saknas delvis standardiserade och definierade rutiner, processer samt en tydlig och praktiskt användbar incidenthanteringsplan gällande informationssäkerhet. EY rekommenderar kommunstyrelsen att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig hantering av frågorna kring informationssäkerhet.*

  Centrala riktlinjer för Södertälje kommuns informationssäkerhet är sammanställda och gällande fr.o.m. den 7 november 2017. De är publicerade och sökbara på kommunens intranät och sprids även genom återkommande särskilda informationstillfällen.

- *Det har bara till viss del påbörjats ett arbete och informationsspridning om EU:s gemensamma dataskyddsförordning (GDPR) som kommer att ersätta personuppgiftslagen (PUL). Det är angeläget att samtliga verksamhetsområden inom kommunens förvaltning hinner anpassa sig till det nya regelverket innan förordningen träder i kraft den 25maj 2018.*

  Ett GDPR-projekt är etablerat och pågående i Södertälje kommun med hjälp av externt expertstöd. Kartläggning och klassning var klart december 2017. Riskanalys och åtgärdsplanering pågår. Åtgärderna implementeras under våren 2018.

  Insatser och åtgärder omfattar bl. a:
  - Säkerställande av ett hållbart informationssäkerhetsarbete genom förbättringar av relevanta styrande dokument, policys, riktlinjer, processer och instruktioner.
  - Centrala resurser används i syfte säkerställa samordning och uppföljning på ett kostnadseffektivt sätt.
  - Central styrning av incidentrapportering, informations- och utbildningsinsatser, personuppgiftsförteckning
  - Nödvändiga förändringar av avtal med leverantörer samt hantering av registrerades rättigheter.
  - Kommunkoncernen samordnar åtgärderna inom förvaltningen och Telge AB.

Beslutsunderlag
Kommunstyrelsens kontors tjänsteskrivelse 19 januari 2018
Revisionsskrivelse informationssäkerhet 2017
Södertälje kommun informationssäkerhetsgranskning 2017 nr 5

Ekonomiska konsekvenser och finansiering
Arbetet med informationssäkerhet kräver personella och ekonomiska resurser. Inom ramen för 2018 års budgetanslag har bl. a medel avsatts för en informationssäkerhetsansvarig som planeras kunna påbörja sin anställning under våren. Resursbehovet för de framtida åtgärder som kan komma att vidtas får prövas i samband med den årliga processen med Mål och Budget och verksamhetsplan/internbudget.

Kommunstyrelsens kontors förslag till kommunstyrelsen:
Kontorets tjänsteskrivelse överlämnas som kommunstyrelsens svar på revisionsrapporten till kommunens revisorer.

Rickard Sundbom
Stadsdirektör

Per Tegel
Säkerhetschef

Beslutet expedieras till:
Kommunens revisorer och akten

Södertälje kommun
Revisorerna

Revisionsskrivelse
2017-11-16

Till: Kommunstyrelsen
För kännedom: Kommunfullmäktige

Revisionsrapport nr 5/2017 – Granskning av informationssäkerhet

På vårt uppdrag har EY genomfört en granskning i syfte att undersöka på vilket sätt kommunen arbetar för att upprätta en god informationssäkerhet. Granskningen har gjorts med hjälp av EYs egna analysverktyg Cyber Program Assessment respektive GDPR Target Assessment. GDPR är den engelska förkortning av EU:s allmänna dataskyddsförordning som träder i kraft 24 maj 2018.

EYs bedömning är att 19 procent av kontrollerna som granskats fungerar tillfredsställande, 53 procent fungerar delvis och 28 procent fungerar inte tillfredsställande alternativt så saknas kontroller som borde finnas på plats.

Av granskningsrapporten framgår att de mest väsentliga riskerna bedöms vara kopplade till följande fem områden:

För det första. Kommunen har betydande delar av sin IT-verksamhet outsourcad. Man gör inte själv några systematiska säkerhetstester utan förlitar sig helt på att leverantörerna håller sina delar av avtalen. Vi rekommenderar därför att kommunstyrelsen inför en process för säkerhetstester samt regelbunden granskning och revidering av avtal.

För det andra visar granskningen att kommunens informationssäkerhetspolicy inte har uppdaterats på tre år, vilket innebär en risk att den inte är anpassad efter förändrade omständigheter i organisationen och i omvärlden. Vi rekommenderar kommunstyrelsen att policyn ses över löpande och åtminstone en gång per år.

För det tredje. Det genomförs inga utbildningsinsatser inom informationssäkerhet. Vi rekommenderar att ett strukturerat utbildningsprogram genomförs.

För det fjärde. Det saknas delvis standardiserade och definierade rutiner och processer samt en tydlig och praktisk användbar incidentshanteringsplan gällande informationssäkerhet. Vi rekommenderar kommunstyrelsen att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig hantering av frågorna kring informationssäkerheten.

För det femte. Det har bara till viss del påbörjats ett arbete och informationsspridning om dataskyddsförordningen som kommer att ersätts personuppgiftslagen (PUL). Det är angeläget att samtliga verksamhetsområden inom kommunen hinner anpassa sig till det nya regelverket innan förordningen träder i kraft 25 maj nästa år.

Vi önskar kommunstyrelsens synpunkter på vår skrivelse och bifogade granskningsrapport. Svar från önskas senast 2018-01-31

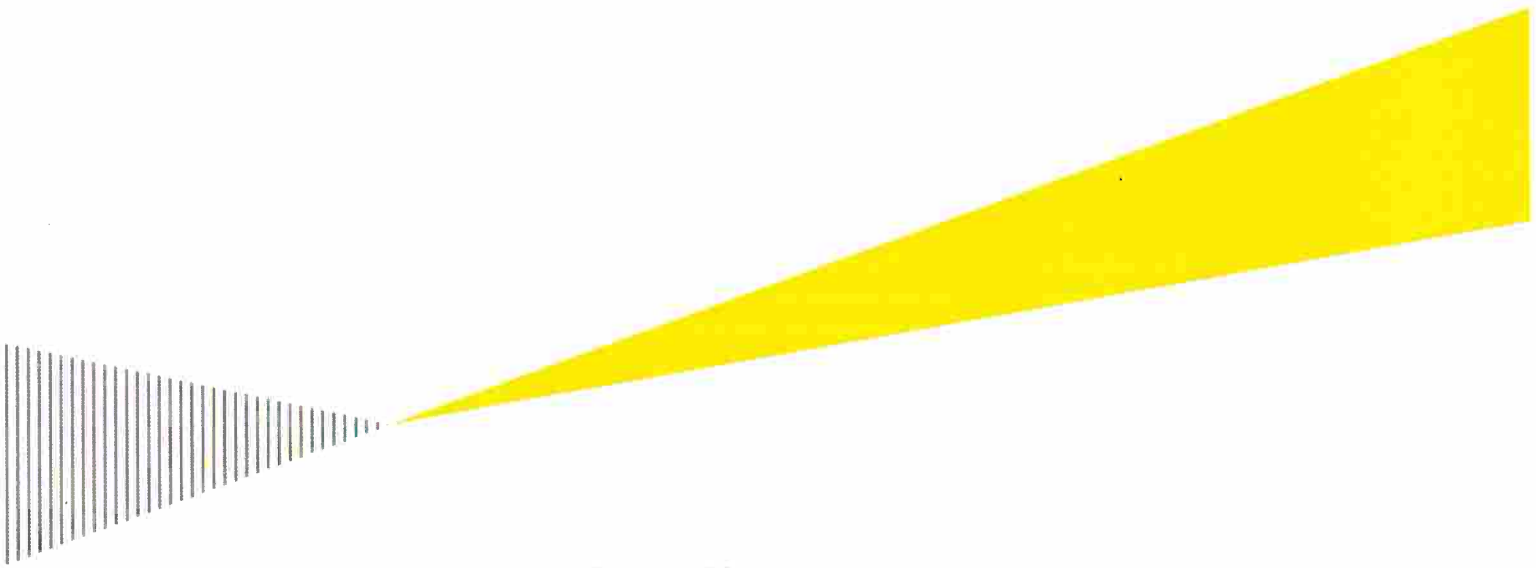
För revisorerna i Södertälje kommun

Christer Björk

Elisabet Komheden

Bilaga: Revisionsrapport nr 5/2017 – Granskning av informationssäkerhet

Revisionsrapport nr 5/2017



Södertälje kommun

Rapport: Informationssäkerhetsgranskning

10 oktober 2017

EY
Building a better working world

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Södertälje har EY genomfört en granskning av informationssäkerhet vad gäller policyer, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå i kommunen. Syftet med granskningen har varit att undersöka på vilket sätt kommunen jobbar för att upprätta en god informationssäkerhet. Granskningen har gjorts mot utvalda delar av EYs ramverk Cyber Program Assessment respektive GDPR Target Assessment.

Övergripande slutsatser

Av samtliga 62 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	19 %
Kontrollen finns och fungerar delvis:	53 %
Kontrollen finns ej eller fungerar ej tillfredsställande:	28 %
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	0 %

Södertälje kommun är delvis en decentraliserad organisation som är beroende av externa leverantörer. På en central nivå hanteras kommunen gemensamma IT-stödet av kommunens IT-enhet. Merparten av alla lärares och elevers användarnära utrustning (datorer, läsplattor mm.) hanteras istället inom respektive rektorsområde. I och med Södertälje kommuns användning av leverantörer finns det ett behov av styrning och uppföljning av dessa för att säkerställa att avtal uppfylls. Eftersom de enskilda kontoren och organisationerna i hög grad själva kan strukturera sina system och sitt IT-stöd, ger det en varierad flora av system, processer och kontroller. Det ger också en varierande grad av mognad i processer och kontroller. Variationer återfanns främst inom uppföljning av IT-leverantörerna där Utbildningskontoret kommit längst då de i dagsläget har regelbundna möten med leverantörerna, om än inte att någon granskning av avtalet sker. Därtill fanns det variationer i hur incidenter hanteras och om det finns rutiner för detta. Dessa variationer berodde delvis på typ av system samt hur många användare det hade, där verksamhetskritiska system hade tydliga processer. Avsaknad av tydlig styrning tillsammans med avsaknad av tydliga, uppdaterade, kommunicerade riktlinjer för hur anställda ska hantera IT kan dessutom utsätta verksamheten för risker med avseende på informationssäkerhet. Södertälje kommuns beroende av externa leverantörer kan också leda till risker för verksamheten om avtal inte följs upp och leverantörer inte tillhandahåller de servicenivåer som överenskommits. En ytterligare orsak till den rådande bedömningen härrör att det i varierande grand finns/saknas en incidenthanteringsplan gällande informationssäkerhet som är övergripande, konkret och praktisk användbar. Därutöver är Södertälje kommun i behov av att praktisk påbörja arbete med den nya dataskyddsförordningen (General Data Protection Regulation GDPR) för att hinna säkerställa sig mot de största riskerna.

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Fullständiga iakttagelser och rekommendationer återfinns i kapitel 4.

	Iakttagelse och rekommendation	Prioritet
1.	Kommunen har delar av sin IT-verksamhet outsourcad. Vissa verksamhetssystemen köps som tjänst direkt från systemleverantören. Kommunen förlitar sig på att leverantörerna håller sina delar av avtalen och genomför inte själva några systematiska säkerhetstester för att identifiera sårbarheter. Samtidigt sker det i flera fall inte någon uppföljning av leverantörerna förutom den granskning som sker då avtalen skrivs under. Det rekommenderas att Södertälje kommun implementerar en process för regelbunden granskning och revidering av avtal.	Hög
2.	Kommunen har inte uppdaterat sin informationssäkerhetspolicy på tre år, vilket innebär en risk att den inte är anpassad efter förändrade omständigheter i organisationen och omvärlden. Policyn är i sådant fall bristfällig och det rekommenderas att den ses över löpande, åtminstone en gång per år. Enligt information är organisationen på gång att implementera vedertagen metod för ledning av informationssäkerhetsarbetet (ISO27000-serien). En sådan implementering skulle hantera flertalet av de frågor som berörs i materialet.	Hög
3.	Kommunen genomför inga utbildningsinsatser inom informationssäkerhet. I och med detta riskerar bristande kunskap och medvetenhet exponera och utsätta organisationen för informationssäkerhetsrisker. Det rekommenderas att ett strukturerat och gediget utbildningsinitiativ startas.	Hög
4.	Kommunen delvis saknar standardiserade och definierade rutiner och processer kring informationssäkerhet, styrning kring dessa samt en tydlig, konkret och praktisk användbar incidentshanteringsplan gällande informationssäkerhet. Det finns dokument med roller och ansvarområden, men det finns en viss avsaknad av en plan innehållande utredning, prioritering, minimering av skador, återhämtning och dokumentering. Styrningen och rutinerna skiljer sig åt i verksamheten. Det rekommenderas att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig informationssäkerhetsbild.	Hög
5.	Kommunen har påbörjat arbete och informationsspridningen om GDPR. System- och informationsägare har kunskap om vad för information som de har och var den finns sparad. Flertalet verksamhetsområden har dock inte påbörjat arbetet i vidare bemärkelse. Det rekommenderas att kommunen tydliggör vad som kommer skötas centralt och vad som förväntas skötas av varje enskild verksamhet. Södertälje kommun måste se till att driva "projektet" GDPR i hamn innan maj 2018, eller åtminstone de mest essentiella delarna.	Hög

Innehåll

1. Bakgrund

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå målen för en kommuns verksamhet krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har tillräckligt starkt skydd och är spårbar.

Inom Södertälje kommun hanteras det gemensamma nätverket med datakommunikation, servrar, så kallade administrativa datorer, telefoner och vissa verksamhetssystem av kommunens IT-enhet. Merparten av alla lärares och elevers användarnära utrustning (datorer, läsplattor mm) hanteras inom respektive rektorsområde. Till sist är det så att flertalet verksamhetssystem köps av verksamheterna som tjänst direkt från systemleverantören. Huvudansvaret är decentraliserat där verksamhetschefen sedan själv, eller genom delegerat ansvar, är systemägare och informationsägare till systemet. Detta innebär att bedömningen över kommunens eventuella gap gentemot god praxis inom informationssäkerhetsstyrning samt gentemot dataskyddsförordningens krav behöver nyanseras och beakta att det kan skilja mellan olika delar av organisationen. Även om vissa aspekter inte ligger under central styrning kan de likväl skötas fullt korrekt.

Det bör noteras att ansvaret för kommunens övergripande informationssäkerhetsarbete har legat hos IT-strategen som varit placerad på stadsdirektörens kansli fram till 161231. Från 170101 har ansvaret flyttats över till Säkerhetsavdelningen som haft visst konsultstöd i avvaktan på rekrytering. När nödvändiga roller är besatta väntas informationssäkerhetsarbetet drivas framåt i full omfattning igen.

1.1 Syfte

Syftet med granskningen har varit att undersöka på vilket sätt kommunen jobbar för att upprätta en god informationssäkerhet. För att besvara granskningens syfte och bedöma kommunens rutiner har granskningen utgått från följande revisionsfrågor:

- Finns en tydlig styrning av informationssäkerhet och IT-säkerhet i kommunen genom tydliga och ändamålsenliga policys och styrdokument? Är dokumenten på övergripande nivå beslutade av kommunstyrelsen?
- Finns en process för strukturerad kontroll och uppföljning avseende att policys och styrdokument efterlevs? Sker dokumenterad återrapportering av styrdokumentens efterlevnad till berörd beslutsfattare för styrdokumenten?
- Finns risker gällande kommunens informationssäkerhet dokumenterade och uppdateras denna dokumentation löpande?
- Finns det en tydlig ansvarsfördelning gällande vem som ansvarar för kommunens informationssäkerhet och vem som ska utföra säkerhetsarbetet?
- Finns säkra rutiner för ändring och avslut av behörigheter?
- Finns det en tillräcklig intern kontroll och följer ansvariga nämnder upp arbetet med informationssäkerhet?
- Får kommunens anställda tillräcklig och ändamålsenlig information gällande IT-säkerhet?
- Finns det någon policy för hur inkomna mejl och sms ska hanteras?
- En översiktlig bedömning av hur Södertälje kommun förbereder sig för införandet av den nya dataskyddsförordningen maj 2018?

1.2 Metod

Revisionsfrågorna har besvarats genom en granskning mot så kallad god praxis inom informationssäkerhetsområdet. Granskningen har gjorts mot utvalda delar av EYs ramverk Cyber Program Assessment samt ur EYs ramverk GDPR Target Assessment. Ramverket bygger på de svenska och internationella standarderna ISO/IEC 27000, COBiT och ITIL.

EY har genomfört en övergripande kartläggning av rutiner, kontroller samt kortfattat behandlat styrningsfrågor rörandes informationssäkerhet. Därtill har EY gjort en övergripande nulägesanalys om var Södertälje kommun står gällande GDPR.

Innan granskningen påbörjades hölls ett initierande möte med Södertälje kommuns säkerhetschef och Södertälje kommuns IT-chef. Under detta möte beskrevs syftet med granskningen, upplägget samt revisionsfrågorna som skulle besvaras. Granskningen genomfördes sedan först via insamling och granskning av information av befintliga styrande dokument. Därefter genomfördes intervjuer med de personer som ansågs kunna ge en fullständig bild över verksamheten, för djupare förståelse för aktuella processer, övergripande rutiner samt verksamma kontroller. Under granskningen har dock inga stickprovstester utförts, vilket innebär att vi inte granskat efterlevnad av dessa rutiner och kontroller. Då Södertälje kommun under denna granskning hade ett pågående arbete med utveckling av riktlinjer för informationssäkerhet har även detta dokument granskats. Dock har det inte tagits hänsyn till vid granskningen. Det eftersom riktlinjerna inte ännu är godkända, varpå de inte spridits inom kommunen och således inte ännu efterlevs.

Under granskningen intervjuades:

- Per Tegel - Säkerhetschef
- Jonas Knutsson – IT-chef
- Eduardo Morris - Kulturstrateg & marknadsansvarig, PUL-ansvarig och har ett IT-ansvar
- Rose-Marie Kellkvist Sundström – Redovisningschef, systemägare kommunstyrelsekontoret
- Mats Nyman – Systemförvaltare, kommunstyrelsekontoret
- Magnus Bergkvist, IKT-Strateg, utbildningskontoret
- Helena Götherfors – Miljökontorschef, systemägare, miljökontoret
- Simon Lindgren - IT Strateg, systemägare, social- och omsorgskontoret,
- Homan Gohari – Tf samhällsbyggnadsdirektör, samhällsbyggnadskontoret
- Anna Nilsson – PUL-ombud

Därefter har denna rapport utformats som underlag för revisorernas bedömning av hur ändamålsenlig informationssäkerheten är i kommunen. Rapporten beskriver vår bedömning av kommunens mognadsgrad per huvudområde samt våra iakttagelser och rekommendationer.

Följande huvudområden har granskats och utvärderats:

- Policyer och styrdokument

- Kontroll och uppföljning av policyer och styrdokument
- IT-leverantörer
- Risker kopplade till informationssäkerhet
- Ansvarsfördelning
- Behörighetshantering
- Intern kontroll
- Information och utbildning
- Policyer/riktlinjer för e-mail och sms
- General Data Protection Regulation (GDPR)

2. Granskning

2.1 Granskningsprotokoll

Följande avsnitt innehåller de frågor som ingick i granskningen samt varje enskild frågas medelvärde erhållet av intervjuerna som genomförts. Utvärderingarnas svar har jämförts med de poängsatta svarsalternativen i EYs ramverk Cyber Program Assessment samt i EYs ramverk GDPR Target Assessment.

Betydelse	Utvärderingspoäng
Kontrollen finns och fungerar tillfredsställande	3,5 - 5
Kontrollen finns och fungerar delvis	2 - 3,4
Kontrollen finns ej eller fungerar ej tillfredsställande:	1 - 1,9

Granskningspunkt		Kommentar	Utvärdering
1 Policyer och Styrdokument			
1.1	Beskriv organisationens policyer för informationssäkerhet	Det finns riktlinjer och policyer tillgängliga på intranätet. Dock råder det ovisshet om vissa policyer och dokuments existens. Därtill finns det inte alltid en god struktur för var och hur verksamhetsspecifika dokument finns sparade. Det rekommenderas att Södertälje kommun skapar gemensamma riktlinjer för tydliggöra spridningen av dokumenten. Informationssäkerhetspolicy Dnr KS 14/93 fastställdes av kommunstyrelsen för tre år sedan och har inte uppdaterats sedan dess. Policyn är på två sidor och definierar Södertälje kommuns övergripande syn på informations-säkerhet, mål och organisationens intention med informationssäkerhet. Därtill finns det två sidor som beskriver vilka dokumentet gäller för hur informations-säkerhetsarbetet ska organiseras. Styrdokumentet som beskriver Södertäljes organisation för IT och ansvar för den generella IT-miljön är beslutat 2004. Det rekommenderas att policy och styrdokument regelbundet ses över, gärna på årsbasis. På utkast finns det en 38-sidig riktlinje för informationssäkerhet.	3
1.2	Vem äger policyer relaterade till informationssäkerhet, standarder och riktlinjer inom organisationen?	Kommunstyrelsen har beslutat om informationssäkerhets-policyn. Fram till 2016-12-31 ägdes detta av IT-strategen som varit placerad på Stadsdirektörens kansli sedan 2012-01-01. Sedan 2017-01-01 ägs policyer av säkerhets-avdelningen. Kommunens verksamheter beslutar sedan själva om andra styrande dokument och riktlinjer, vilka beslutas av olika personer eller avdelningschefer ute på kontoren. För de olika områdena ansvarar respektive.	4
2 Kontroll och uppföljning av policyer och styrdokument			
2.1	Finns en process för strukturerad kontroll och uppföljning avseende att policyer och styrdokument efterlevs?	Det finns en inte någon process för strukturerad kontroll och uppföljning avseende policyers och styrdokuments efterlevnad.	1
2.2	Har ni en (acceptabel) användarpolicy för epost och Internet?	Södertälje kommun använder sig av det tvåsidiga dokumentet "Användarförsäkran" Dnr KS 16/179 beslutad 2016. Denna beskriver hur Södertälje kommuns datorer, andra digitala enheter, internet, lösenords och behörigheter får användas. Flertalet intervjuade verkar dock inte ha vetskap om dokumentet. Därutöver, användarna av administrativa datorer får då de startar dessa information om att datorn är Södertäljes egendom samt hur datorn får användes. Detta gäller dock inte lärar- och elevdatorer.	2
2.3	Har ni en process för versionskontroll av integritetspolicyer och notiser/meddelanden?	Policyer diarieförs när de är beslutade. Det finns dock brister i denna dokumentation, där exempelvis Inköpspolicyn varken har diarienummer eller ett godkännande. Andra styrdokument och riktlinjer som beslutas på lägre nivå finns det ingen versionskontroll av. För dessa är det ej heller alltid tydligt vem som skrivit eller godkänt dem. Ej heller är de enhetligt skriva eller sparade.	4
2.4	Har beslutande organ godkänt integritetspolicyn?	Kommunstyrelsen har godkänt integritetspolicyn. Sedan årsskiftet 2017 ägs policyer av säkerhetsavdelningen	5
3 IT-leverantörer			
3.1	Hur använder ni er av leverantörer?	Kommunen använder leverantörer för alla sina system och IT-tjänster. Telge Inköp AB måste enligt Södertälje kommun Inköpspolicy vara inkopplade om inköpet är omkring 284 00 kr minimum. Telge Inköp AB hjälper då till att skriva och granska avtal. Emellanåt måste dock Södertälje kommun följa leverantörernas avtal. Vid dessa tillfällen granskas det att Södertäljes minimumkrav åtminstone finns med.	4

3.2	Hur hanteras avtal med leverantörer?	Telge Inköp AB hjälper till med upphandling av avtalen och avtalstecknande. Det är sedan upp till varje chef/systemansvarig att se till att avtalen följs. Det råder variation bland kontoren i hur avtalen hanteras och följs upp.	3
4 Risker kopplade till informationssäkerhet			
4.1	Finns en formell grupp för informationssäkerhets-incidenthantering?	Det råder divergerade uppfattningar här. På övergripande nivå finns säkerhetsavdelningen, sedan finns det till viss delinformella grupper för incidenthantering, men det saknas instruktioner för hur incidenter ska behandlas. De intervjuade har inte kunnat beskriva någon central formell process för hantering av informationssäkerhetsincidenter där det har framkommit att incidenthanteringen och riskbedömning sköts och sker på olika sätt. För den delen som är outsourcad av IT-enheten finns formella incidentprocesser kopplade till leverantörer.	3
4.2	Har organisationen ett dokumenterat och implementerat program för integritetsincidenter och hantering av brott och identifiering av misstänkta brott samt hantering av dem?	Det finns ingen obligatorisk utbildning kring hantering av informationssäkerhetshantering och processerna kring detta är inte väl spridda genom kommunen.	2
4.3	Vad är omfattningen och strategin för övervakning av säkerhet inom organisationen?	Övervakningen är till stor del överlämnad till leverantörer. Den övervakning som sker inom kommunens enheter är ad hoc. Det finns ingen utnämnd person inom Södertälje kommun som är ansvariga för övervakning av säkerhet inom organisationen. Säkerhetsfrågor hanteras istället av respektive verksamhet och t ex av IT-enheten själva.	2
4.4	Beskriv organisationens modell för översyn och strategisk ledning av (programmet för) övervakning av säkerhet?	Enheterna har olika tillvägagångssätt för att hantera övervakningen och hålla ledningen informerad, vilket sker i olika grad. Större delen av driftverksamheten ligger dock hos leverantörer utanför Södertälje kommun och det saknas tillräcklig uppföljning av dessa. Det finns ingen specifik avsatt budget för övervakning av säkerhet. Enligt intervjuer ska övervakning skötas åtminstone delvis på decentraliserad nivå.	2
5 Ansvarsfördelning			
5.1	Finns definierade roller och ansvar för informationssäkerhetsarbetet?	Södertälje kommun är en decentraliserad organisation. Det finns definierade roller och ansvar kring informations-säkerhet men det saknas i dagsläget personal för att fylla rollen som informationssäkerhetschef. Rollen som systemansvarig och rollen som informationsägare behöver tydliggöras ute i verksamheten så att alla uppfattar dem på samma sätt och inte som idag att bara en del har uppfattat rollerna	3
5.2	Hur drivs arbetet med informationssäkerhet i organisationen?	Informationssäkerhet drivs från olika håll. Leverantörerna handhar mycket av ansvaret. Hos Södertälje finns inget tydligt detekterat team som hanterar den dagliga informationshanteringen. Driften ägs och utfärdas oftast av centrala grupper inom verksamhetsområdena.	3
5.3	Finns en grupp dedikerad till övervakning av säkerhet?	På grund av den decentraliserade organisationen finns det ingen grupp dedikerad till övervakning av säkerhet. Leverantörerna handhar mycket av övervakningen. Systemansvarige är ansvariga för informationen gällande system. Övervakning av säkerhet benämns inte. Systemägarna/informationsvägarna har i vissa fall enbart grundläggande och inte någon djup kunskap om säkerhetsövervakning.	2

6 Behörighetshantering			
6.1	Beskriv de standardiserade processer som finns för behörighetshantering.	Det finns en standardiserad process vad gäller IT-enhetens ansvar för användarkonton till miljön som helhet vilket styrs av HR-systemet och IT-enhetens behörighetssystem Däremot så finns inte någon standardiserad process för hur respektive verksamhetssystem hanterar behörigheterna inom sina respektive system. De har sina respektive processer. Rutiner existerar av olika grad för de olika systemen. Brister finns inom borttag av behörigheter där det idag på flera ställen saknas både standardiserande och etablerade processer.	2
6.2	Hur skapas behörigheter?	Det beror på system och systemägare. Det är blandat mellan rollbaserat och inte rollbaserat vilket ger utmaningar i informationssäkerhetsarbetet. Någon granskning av processen sker inte på regelbunden basis.	4
7 Intern kontroll			
7.1	Vad är omfattningen och strategin för övervakning av säkerhet inom organisationen?	Majoriteten av Södertälje kommuns IT-verksamhet är outsourcad och verksamhetssystem köps huvudsakligen som tjänst. Undantaget är skol-IT. Strategin bygger till stor del på att förlita sig på kommunens leverantörer. Dock finns det kontor och verksamheter som påbörjat arbetet och har etablerat en monitoreringsstrategi och informationskartläggningar.	2
7.2	Beskriv organisationens kontroll och styrning av strategin av övervakningsprogram?	Södertälje kommun förlitar sig på deras leverantörer för översyn och strategisk ledning för övervakning av säkerhet. Telge Inköp AB bedriver inköpsverksamheten i form av upphandlingar, tecknande av ramavtal och utveckling av inköpsprocesser, varpå inköpsprocessen är centralt styrd. Kommunens ledning har idag ingen kontinuerlig, aktiv eller konsekvent involvering i säkerhetsövervakningen.	2
7.3	Beskriv organisationens strategi för informationssäkerhet. Hur ofta granskas strategin för informationssäkerhet och av vem?	Det finns ingen skriftlig eller kommunicerad Informationssäkerhetsstrategi innehållande mål, aktiviteter för hur informationssäkerheten ska styras eller bedrivas. Dock finns det en vision och strategi för hur IT ska möjliggöra Södertälje kommuns samhällsutveckling. Visionen gäller för 2009.	2
7.4	Har ni ett program för identifiering av attacker/intrång (t.ex. APT)?	Inget program för identifiering av attacker/intrång finns i nuläget.	3
7.5	Beskriv organisationens hantering av hot och sårbarhet, innefattandes tilldelning av ansvar samt rapportering till kommunstyrelsen.	Det finns inga formella rutiner för hantering av hot och sårbarhet. Kommunen förlitar sig på leverantörer för hantering av hot och sårbarhet. Avdelningarna hanterar detta på olika sätt, genom ex. SMART-analyser och riskanalyser.	2
7.6	Beskriv er strategi för att definiera en lämplig omfattning när ni genomför en attack- och penetrationsbedömning mot en grupp tillgångar.	Södertälje utför inga egna tester utan förlitar sig på deras leverantörer och att leverantörerna utför det.	2
7.7	Hur utvärderas hot mot nya och framväxande teknologier (t.ex. molnlagring och BYOD)?	Det råder diversifierade uppfattningar om hanteringen kring detta. För vissa kontor framhålls utvärderingen vara bristfällig. För andra kontor framhålls den istället vara mer tillräcklig då riskanalyser utförs och rapporteras. IT-enheten kan innan nya tjänster eller teknologier upphandlas göra bedömningar och certifieringar.	3
8 Information och utbildning			
8.1	Är informationssäkerhetsutbildning obligatorisk för samtliga användare då de börjar arbeta i organisationen?	I nuläget finns det ingen informationssäkerhetsutbildning för samtliga användare i kommunen. Det är upp till varje avdelningschef att informera och utbilda personalen om detta.	1
8.2	Finns program för medvetenhet om säkerhetsfrågor som täcker hela organisationen?	I nuläget finns det inget program för medvetenhet om säkerhetsfrågor som täcker hela organisationen.	1

8.3	Hur sprids säkerhetspolicyer, standarder och riktlinjer inom organisationen?	Säkerhetspolicyer och riktlinjer sprids via intranätet. De läggs upp där för varje medarbetare att själva hämta hem. Specifika riktlinjer sprids på respektive kontor via olika kanaler. På kontoren saknas det formaliserade rutiner då organisationen är beroende av enskilda individers initiativ för att dessa ska spridas.	2
8.4	Hur kommuniceras strategin för informationsstrategi inom organisationen?	Det finns en strategi för vad kommunen kan uppnå med IT. Visionen är dock för mål att uppnå för 2009. Visionen är inte heller väl kommunicerad till medarbetare inom kommunen.	2
9 Policyer/riktlinjer för SMS och mejl			
9.1	Finns formella policyer och riktlinjer för säkerhet kring hantering av SMS, mejl m.m. etablerade och kommunicerade till hela organisationen?	Det finns formella policyer for informationssäkerhet (2014), riktlinjer för hantering av mobiltelefoner (2012 - ej sms), trådlösa nät (2013- ej till slutanvändare) hantering etc. Dessa är dock bristfälliga och heller inte väl uppdaterade. Det håller på att tas fram riktlinjer för informationssäkerhet som uppfyller SS-ISO/IEC 27000-serien.	3
9.2	Finns formella processer etablerade för hantering av SMS m.m.?	Det finns inga formella processer etablerade för hantering av SMS. Det finns dock en användarpolicy (2016) för hur telefonsamtal, dator, mobil, surfplatta ska användas. EMM-system har implementerats i vissa telefoner som låser in information i telefonen och låter administratörer låsa/radera telefonen remote.	2
10 General Data protection Regulation (GDPR)			
10.1	Finns ett uppgiftsskyddsombud (Data Protection Officer)?	Det finns inte någon anställd med denna roll i nuläget. Kommunen har dock planer på att tillsätta en DPO.	2
10.2	Finns det specifika regler, processer och verktyg för att möjliggöra effektiv hantering av sekretess och informationsintegritet?	Kommunen har processer och regler, men inte standardiserad utbildning för nyanställda. Materialet sprids inte på ett effektivt sätt och därmed finns inte möjlighet att säkerställa att lagar och regelverk efterlevs.	3
10.3	Har ni en sekretess/integritetspolicy?	Kommunen har användarinstruktioner för hur känslig information ska hanteras.	3
10.4	Finns det krav på att anställda känner till, följer samt godkänner sekretesspolicyn?	Nej. Det finns inget krav på godkännande. Anställda förväntas att följa rådande lagar och regelverk.	1
10.5	Har ni en användarpolicy för e-post och internet?	Södertälje kommun har skriftliga instruktioner för hur e-post och internet ska användas. I "Användarförsäkran" (2016) beskrivs regler för hur bl.a. digitala enheter och internet får användas. Anställda har dock inte god kunskap om dokumentens existens.	5
10.6	Finns det en definierad process för identifiering av affärsprocesser som använder, samlar in, arkiverar, kasserar och inkluderar avslöjande av personlig information?	Södertälje har en användarinstruktion för hur känslig information ska hanteras. Södertälje kommun har även instruktioner för informationsklassning. Detta dokument innehåller bl.a. ofta förekommande tillämpbara lagar samt hur information i ett system ska klassificeras och behandlas.	5
10.7	Är dataskydd en del av riskbedömning och rapportering?	Riskbedömningar görs vid inköp av nya system. Generellt saknas en väletablerad process för detta.	1
10.8	Utför er organisation Data Protection Impact Assessments (DPIA) för att bedöma risker för nya projekt eller system?	Vid inköp av nya tjänster eller teknologier kontaktas IT-enheten som då bl.a. gör bedömningar på risker och inverkan.	4
10.9	Genomförs insatser för att kommunicera med dataobjekt (t.ex. anställda eller kommunmedborgare) kring hur personinformation används då den samlas in (t.ex. via utskick)?	Samtycke tas i samband med insamling av personuppgifter. Södertälje kommun har flertalet personuppgiftsombud som kontrollerar att personuppgifter behandlas på ett korrekt och lagligt sett. Inga generella insatser görs. Det finns styrande dokument som beskriver vad som får kommuniceras och hur. Utbildning är upp till varje chef att genomföra.	4

10.10	Har ni fastställda perioder för kvarhållandet av persondata?	Kommunstyrelsekontoret har en dokumenthanteringsplan för det. Beroende på vad för persondata det är och avsikten med kvarhållandet finns de (enligt rättslig grund) sparade i olika långa perioder. Hur kvarhållandet sedan ska tolkas givet GDPR som kommer att träda i kraft maj 2018 är för vissa systemägare osäkert.	5
10.11	Finns det riktlinjer eller förfaranden för radering av persondata? (Om ja, vänligen beskriv de processer som finns på plats för detta)	Det saknas ett centralt stöd för detta. Uppfyllnad av säkerhetskrav är upp till varje enskild systemägare samt hur det är kravställt vid upphandling och avtalat.	1
10.12	Finns det processer för säkerställandet av dataobjekts rättigheter, t.ex. ämnesförfrågningar, rätten att modifiera data samt rätten att motsätta sig processandet av data?	Det saknas ett centralt stöd för detta, uppfyllnad av säkerhetskrav är upp till varje enskild systemägare samt hur det är kravställt vid upphandling och avtalat.	1
10.13	Har era informationssystem tillräckliga revisions- och spårbarhetsfunktioner för att kunna producera detaljerad information, som även bör finnas tillgänglig på användares begäran, kring vilka källor som används samt användandet av deras personuppgifter?	Det saknas ett centralt stöd för detta, uppfyllnad av säkerhetskrav är upp till varje enskild systemägare samt hur det är kravställt vid upphandling och avtalat.	1
10.14	Vilka kontroller finns för att autentisera användare som har åtkomst till system som används för att processa persondata (t.ex. tvåfaktorsautentisering)?	Varierar från system till system. Den vanligaste kontrollen är ID och lösenord. För vissa system och områden finns även tvåfaktorinloggning.	3
10.15	Vilka lösenordskrav finns till de system som används för att processa persondata, inklusive: - minimumkrav på längd - komplexitet - tvingad återställning - låsning vid misslyckade inloggningsförsök - låsningsgräns - ålder på lösenord - inaktivitet - lösenordshistorik	Detta varierar beroende på system.	3
10.16	Hur skyddas den fysiska åtkomsten till persondata? (t.ex. punktskydd eller skalskydd för lokaler)	Detta varierar beroende på system hur det är kravställt vid upphandling och avtalat.	2
10.17	Har ni en krypteringspolicy eller process?	Det finns ingen central policy. Kravställandet sköts av respektive systemägare samt i upphandlingen via Telge Inköp AB	2
10.18	Har ni ett informationssäkerhetsteam?	Finns roller med informationssäkerhetsansvar men inte ett dedikerat team. Säkerhetsavdelningen är sedan 170101 ansvarig för säkerhetssamordningen. Informationsägare och systemägare samt kontorschef är ansvariga för den faktiska informationssäkerheten för respektive system. Säkerhetsavdelningen genom deras roll som samordnare ansvarar för att respektive informationssäkerhetsansvarig arbetar på ett strukturerat sätt utifrån kommunen policy, riktlinjer och instruktioner.	2
10.19	Tillhandahåller ni en lista med de legala krav kring dataskydd ni är skyldiga att följa?	Nej.	1

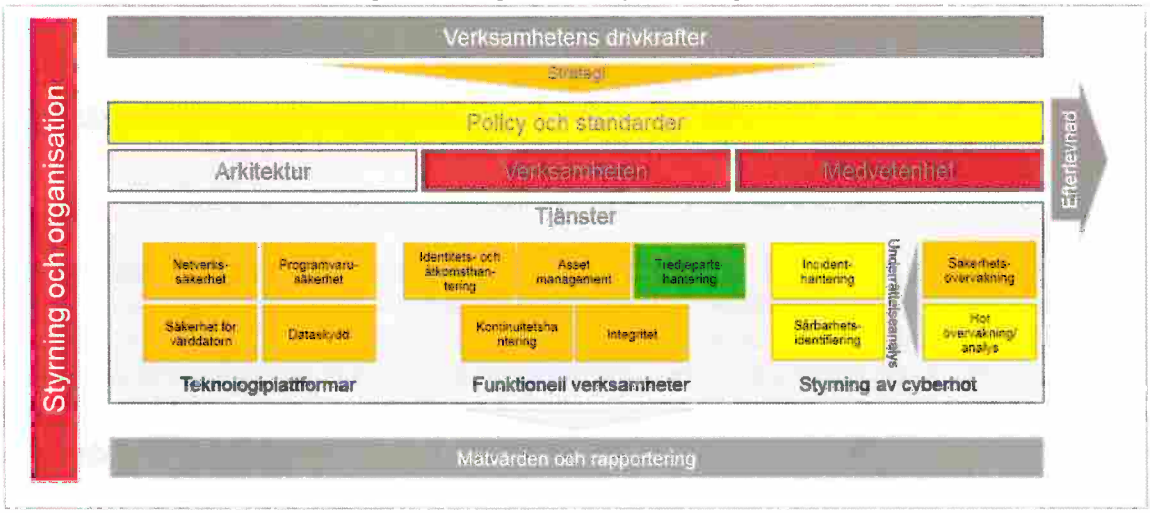
10.20	Är Datainspektionen informerade om persondata som processas?	Nej.	1
10.21	Har ni ett program för att säkerställa att ni följer policyer, regleringar och andra skyldigheter rörande användandet samt skyddandet av persondata?	Nej.	1
10.22	Har ni rapporterat några fall då ni inte efterlevt dataskyddslagstiftning till Datainspektionen under de senaste 12 månaderna?	Nej.	5
10.23	Har ni dokumenterat det juridiska underlaget för hantering av persondata?	Arbete med GDPR har endast påbörjats. Hanteringen av persondata följs till stor del genom kravställning på leverantörerna.	2
10.24	Har ni en dokumenterad process för rapportering och respons till potentiella incidenter angående persondata?	Det finns ingen generell dokumenterad process för detta. Vissa nämnder har ärendehanteringssystem för rapportering och incidenthantering. IT-enheten har genom sina avtal processer för sina system.	1
10.25	Har ni en responspolicy kring informationsbrister med utsedda ansvariga?	Nej.	1
10.26	Vilka steg tas för säkerställandet av leverantörers efterlevnad av lagar och regelverk för dataskydd?	I kontrakten står det de regler och lagar som leverantören är skyldig att uppfylla. Generellt finns det ingen uppföljning på om och hur detta efterlevs. I vissa fall hålls möten med leverantören där det sker muntlig kommunikation kring detta.	2
10.27	Inkluderas dataskyddsklausuler i kontrakt med leverantörer? (detaljerat svar)	Telge Inköp AB hjälper till med kontakt och upphandling. Kontrakt varierar från system till system.	4
10.28	Hur genomförs den kontinuerliga bedömningen av leverantörers efterlevnad av dataskyddslagsstiftning?	Generellt sker det ingen kontinuerlig bedömning.	1
10.29	Har ni granskat kontrakt med leverantörer för att avgöra huruvida förändringar eller ytterligare avtal krävs för att efterleva de nya kraven för datahanteringsavtal?	Nej.	1
10.30	Finns det en specialiserad utbildning om personinformation?	Nej.	1
10.31	Hur säkerställs anställdas förståelse kring dataskyddsåtaganden?	Under våren 2017 var Säkerhetsansvarig samt en konsult och informerade de olika kontorens ledningsgrupper. Det finns även möten. En grupp har satts samman vilken ska samordna informationssäkerhetsarbetet och GDPR. Det råder dock diversifierad inställning till hur denna grupp bedrivs för att säkerställa förståelsen för de åtagande som måste göras. Åtaganden ligger till stort på systemägarna.	3
10.32	Hur kommuniceras åtaganden rörande dataskydd till nyanställda?	Viss information finns passivt tillgängligt på intranätet. Liksom för övriga viktiga områden är det idag upp till anställande chef att säkerställa att nyanställda får rätt information utifrån vad man jobbar med. Specifikt för GDPR finns inte. Möten har skett under våren för att informera chefer om dess innebörd. Nyanställda har dock inte fått tillgång till informationen	1

3. Nulägesanalys avseende informationssäkerhet samt bedömning avseende dataskyddsförordningen (GDPR)

Nedanstående bild visar en sammanställning av resultaten av de kontroller som genomförts under granskningen. Dessa kommer ifrån EY Cyber Program Assessment som är baserat på den svenska och de internationella standarderna ISO/IEC 27000, COBiT och ITIL. Diagrammen är färgkodade enligt följande:

- Grön representerar kontroller som fungerar tillfredsställande
- Gul och orange representerar kontroller som fungerar delvis
- Röd representerar kontroller som inte finns eller fungerar inte tillfredställande
- Grå representerar kontroller som inte är använda i denna granskning

Bild 1: Bild visade sammanställning av Södertälje kommuns anpassning till ISO/IEC 27000, COBiT och ITIL efter granskning via EY Cyber Program Assessment tool.



Ur bilden går det att se att leverantörshanteringen är den mest uppfyllda kontrollen. Detta beror på att Telge Inköp AB är med och säkerställer processen. Samtidigt är det också inom detta område som förbättring finns att genomföra, vilket handlar om uppföljning av kontrakt.

Förutom granskningen av informationssäkerhetsstyrningen ställde även ett antal frågor rörandes uppfyllnaden av kraven från den kommande dataskyddsförordningen (GDPR). Följande diagram illustrerar resultaten av dessa frågor.

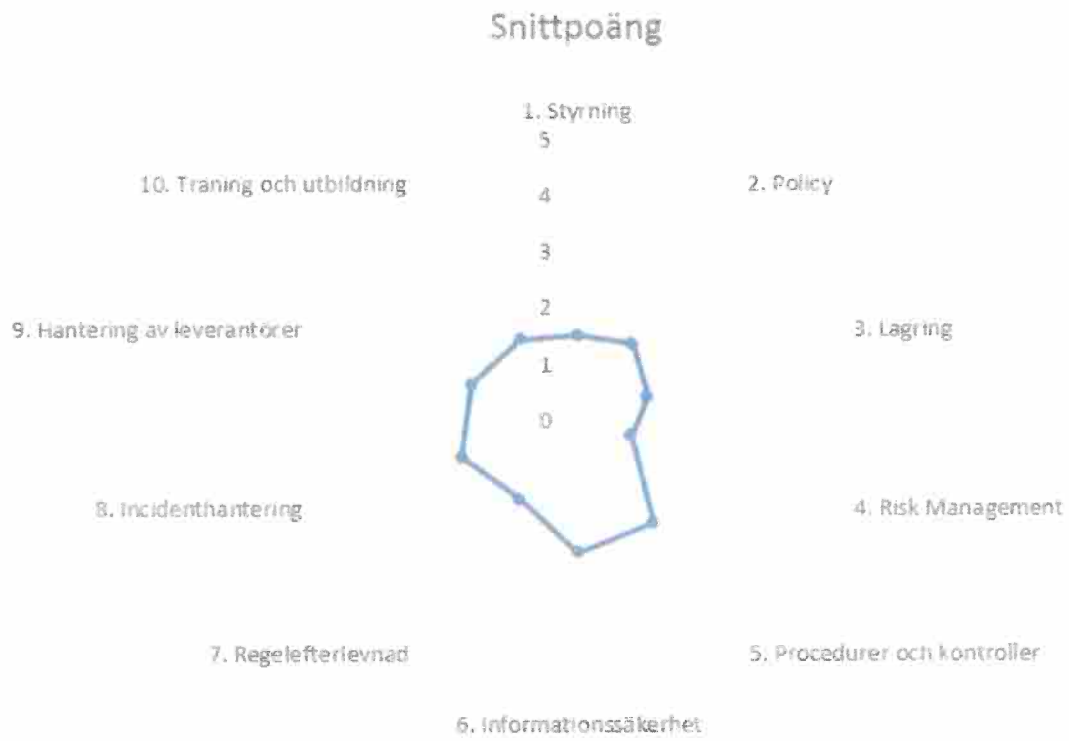


Diagram 1: Spindeldiagram visande Södertälje kommuns adaption till GDPR augusti 2017 givet tio granskningsområden

I spindeldiagrammet går det att se att Södertälje kommuns starkaste områden ligger inom informationssäkerhet och kontroller. Bristerna finns främst inom regelefterlevnad, styrning och riskhantering. Resultatet från diagrammen utgår främst från frågorna under sektion 10 som täcker dataskyddsförordningen (General Data Protection Regulation - GDPR) i granskningsprotokollet i sektion 2.1, men även frågor som berör incidenthantering och policy. Resultatet med dess brister ligger dock i linje med många andra aktörer på marknaden under hösten 2017.

4. Slutsatser och rekommendationer

4.1 Slutsatser

Av samtliga 62 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	19 %
Kontrollen finns och fungerar delvis:	53 %
Kontrollen finns ej eller fungerar ej tillfredsställande:	29 %
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	0 %

Hur ändamålsenlig är informationssäkerheten för de behov kommunens verksamhet har?

I nuläget finns det brister inom några av de granskade områdena. Det pågår initiativ för att förbättra styrning och kontroll inom dessa. Förutsättningar för att nå ett effektivt och ändamålsenligt arbete kring informationssäkerhet finns således hos kommunen. Södertälje kommun har policy och riktlinjer (kommande) vilka berör många av områdena angående informationssäkerhet. Kommunen har definierade roller och beskrivningar för dess innebörd. Dock framgick det att vissa system- och informationsägare inte är väl medvetna om vad rollerna betyder gällande informationssäkerhet. Vad gäller GDPR och svaren på dessa frågor genererar de i dagsläget låga betyg, vilket är fullt naturligt i och med att arbetet inte påbörjats ännu.

Vid gruppering av IT-enheten, Skol- och utbildningsenheten, och övriga intervjuade enheter återfinns gemensamma starka sidor. Dessa starka sidor som kommunen har gällande informationssäkerhet finns främst dels inom området leverantörer, vilket grundar sig ur att Telge Inköp AB med deras stöd bidrar till att säkerställa processen och upprätthålla effektiva och ändamålsenliga villkor. Dock framkom det att Södertälje kommun ibland måste foga sig till leverantörernas villkor, men dock aldrig så pass att Södertälje kommun måste släppa på viktiga krav. Kommunen har även generellt sett starka och goda kunskaper om hur personlig data ska hanteras, identifieras, klassificeras och kommuniceras.

Dock finns en generell brist kring utbildning och information av informationssäkerhet. Kontorscheferna har t.ex. en pärm som de går igenom tillsammans med den nyanställde. Därefter finns det ingen ytterligare information.

Vad specifikt gäller utbildningskontoret är de aktiva beträffande kontinuerliga möten med de större leverantörerna samt att de har tilldelade roller gällande incidenter (om än inofficiella). På utbildningskontoret sker kontinuerlig granskning av policyer och styrdokument (inklusive registervård). Dock efterlyses styrning från någon central IT-strateg eller informationssäkerhetschef som ser till att alla kontoren gör på samma sätt. Accesser och behörigheter styrs med hjälp av roller i Lärarplattformen. Denna plattform driftas externt, där de var på väg att implementera regelbundna kontroller av den externa parten. Denna kontroll har dock avstannat i väntan på centrala direktiv för hur detta ska skötas. Det finns inarbetade incidenthanteringsprocedurer, man kontaktar den som är ansvarig för systemet i fråga, dock är det osäkert om något är nedskrivet någonstans, och det finns ingen formell incidenthanteringsfunktion på utbildningskontoret(avtalen med

externa parter reglerar deras ansvar vid incidenter). Den intervjuade på utbildningskontoret ser en tydlig risk med den centraliserade strukturen på organisationen och det är att man lokalt stannar av och väntar på centrala direktiv för olika aktiviteter. Vad gäller övervakning av säkerhet varierar det per skola, vilket innebär att man skulle behöva intervjua alla skolor för att få en detaljerad bild över just denna aspekt.

Säkerhetspolicys, standards och riktlinjer sköts för utbildningskontoret på samma sätt som för större delen av övrig verksamhet. Respektive chef sätter själv ev. upp utbildning att gå igenom, och dokumentation får man som regel själv leta reda på i intranätet. Vad gäller policyer för t.ex. sms och telefonmeddelanden osv finns inga direkta policys, men här används EMM som ett verktyg för att åtminstone kunna rensa och nollställa datorer och Ipads mellan utbildningspass. Detta används även för samordning av licenshantering.

Vad gäller GDPR och utbildningskontorets domän har man bra koll på den information som hanteras i de system som används, dock har man mindre koll på all information som sparas utanför "systemet". De har inget dataskyddsombud, och de uttrycker att de behöver centrala direktiv för vad som ska göras.

En styrka avseende den centrala IT-enheten i jämförelse med de andra är framför allt inom deras förståelse av vad rollen systemägare respektive informationsägare är, men även att de i likhet med utbildningskontoret har roller som kan hantera incidenter samt att de inför inköp av nya tjänster och/eller teknologier genomför certifieringar och bedömningar. Brister finns främst inom uppföljning av leverantörer vad gäller informationssäkerhet.

De övriga intervjuade enheterna har i likhet med IT-enheten brister inom uppföljning inom informationssäkerhet av deras leverantörer. Vad sedan gäller denna grupp framkom det att det fanns skillnader sinsemellan beroende hur verksamhetskritiskt och informationskänsligt systemet är och hur många användare det har. I stort sett saknades det för flertalet enheter skriftliga processer och rutiner för incidenthantering samt rutiner för genomförande av riskanalyser och riskbedömningar. Därtill framkom det att det en varierande grad av förståelse kring vad rollen informationsägare och systemägare implicerar.

4.2 Rekommendationer

Nedan följer våra rekommendationer samt vårt förslag på prioritering utifrån bedömd risk och väsentlighet. Rekommendationerna är prioriterade enligt följande:

Hög	Observation av kritisk karaktär som kan riskera kommunens möjlighet att driva verksamhet eller leda till materiella förluster för kommunen. Observation som graderas som "hög" bör omedelbart åtgärdas.
Medel	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, finansiell information, materiella tillgångar och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av kommunens resurser. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre fel i information, mindre brister i efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

ID	Iakttagelse och rekommendationer	Prioritet
1.	**Kommunen förlitar sig på leverantörerna gällande säkerheten av systemen utan att kontrakt följs upp eller granskas.** Kommunen genomför ex. 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. **Risk** Om kontrakt och avtal och teknisk säkerhet inte följs upp och om kommunen inte själva utför tester medför det risker för otillräcklig informationssäkerhet. **Rekommendation** Införa regelbundna leverantörsgranskningar (tekniskt och avtalsmässigt). Att granska och se över avtal med leverantörer är ett essentiellt steg för att vara förenlig med GDPR.	Hög
2.	**Kommunen har inte uppdaterat sin informationssäkerhetspolicy** Policyn förförfattades för ca 3 år sedan och har inte uppdaterats sedan dess. **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** Uppdatera policyn kontinuerligt så att den reflekterarar organisations nuvarande behov och omvärldens möjligheter och krav. Därtill rekommenderas det att Implementera ett ledningssystem som säkerställer att verksamheten aktivt jobbar med styrning och kontroll av verksamhetens informationssäkerhetsarbete.	Hög
3.	**Kommunen genomför inga utbildningsinsatser inom informationssäkerhet** Det saknas ett strukturerat utbildningsprogram inom organisationen för att säkerställ adekvat kunskapsnivå inom informationssäkerhet. **Risk** Utan utbildning kan brister uppstå avseende medvetenhet kring informationssäkerhetsfrågor, vilket kan utsätta organisationen för flertalet risker. **Rekommendation** Det rekommenderas att kommunen startar ett utbildningsinitiativ för att öka och regelbundet säkerställa medvetenheten samt kunskapsnivåerna för att på så sätt minska risken för informationssäkerhetsbrister	Hög
4.	**Gällande informationssäkerhet saknar kommunen en konkret incidentshanteringsplan** Kommunens processer och rutiner för säkerhetsriskhantering och incidenthantering är decentraliserade och styrs av skilda kontor. **Risk** Vid eventuella brister eller incidenter rörande informationssäkerhet kan inte personal rapportera och påbörja åtgärder som processen föreskriver. **Rekommendation** Kommunen rekommenderas att implementera en konkret och praktiskt användbar incidenthanteringsplan.	Hög
5.	**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. **Risk** Utan tydliga instruktioner, resurser och central styrning av övergångsarbetet finns det en risk att organisationen inte fullt ut kommer efterleva nya regelverket. **Rekommendation** Kommunen rekommenderas att påbörja arbetet med GDPR för att se över eventuella gap och i förlängningen säkerställa full efterlevnad av det nya regelverket. Specifikt ses initiativ inom utbildning, granskning av leverantörer, riktlinjer och processer för rapportering som områden med behov av mer resurser och medvetenhet.	Hög

ID	Iakttagelse och rekommendationer	Prioritet
6.	**Kommunen saknar centrala befattningar som innehar en överblick kring informationssäkerhetsarbetet och förvaltningen kring det** Kommunen har i nuläget roller med ansvar inom informationssäkerhet. Det saknas en informationssäkerhetsansvarig för verksamheten som utarbetar planer och riktlinjer kring informationssäkerhet samt ser över förvaltningen. Det finns en central avdelning som äger frågor kring informationssäkerhetsarbete och driver de fullt ut - med t.ex. kompletta rutinbeskrivningar samt etablering av behörighetsadministrationsprocesser, men den saknar permanent bemanning. **Risk** Utan en dedikerad funktion med rätt bemanning saknas medarbetare som innehar en komplett bild av kommunens informationssäkerhet. Risken finns att rutiner och processer är inkompletta och orsakar brister i säkerheten. **Rekommendation** Tillsätt en funktion/roll eller skapa en grupp eller avdelning som fullt ut äger informationssäkerheten och ansvarar för att organisationen följer de riktlinjer och policyer som etableras.	Medel
7.	**Ansvariga behöver medvetandegöras om deras roller och ansvar.** Betydelsen av, och ansvaret som system- och informationsägare finns nedtecknat i flertalet dokument, men full förståelse för vad dessa roller innebär saknas i delar av verksamheten. **Risk** Om inte full förståelse innehas kan det äventyra kraven på insyn, tillgänglighet och säkerhet. Därtill kan det bidra till att kommunen inte fullt ut kommer hinna efterleva GDPR då det i dagsläget är förlagt till Systemägare och Informationsägare att på ett decentraliserat sätt påbörja arbetet. Det kan förstås även leda till att uppgifter som ingår i respektive roll inte blir utförda korrekt. **Rekommendation** Det rekommenderas att ansvaret och innebörden som systemägare-informationsägare förmedlas så att berörda parter tydligt får insikt förväntningar på respektive roll, och hur åtgärder för att säkra informationssäkerhet kan vidtas. En etablerad och enhetlig terminologi inom organisationen underlättar arbetet med rollhantering	Medel
8.	**Det saknas standardiserade rutiner för hur policy, riktlinjer och styrdokument ska utformas, sparas, följas upp och spridas.** Kommunen har i dagsläget policy och styrdokument som är beslutade av olika organ, de är datummässigt ouppdaterade samt sparade i olika format. Vad gäller avdelningsspecifika dokument är det inte tydligt vem som beslutat dem. Det finns inte heller någon kontinuerlig uppföljning av dem. **Risk** Om policy och riktlinjer inte är adekvata kan de inte vägleda till ett effektivt resursutnyttjande för verksamheten som helhet. Inte heller kan det främja en ömsesidig förståelse och efterlevnad hos personal. **Rekommendation** För varje policy bör den utredas hur den kan efterföljas i praktiken och hur kontrollen av detta sker. Beroende på typ av policy bör detta ske med olika tidsintervaller. IT-policy rekommenderas att granskas på årsbasis. Utifrån t.ex. implementering av ett ledningssystem för informationssäkerhet skulle processer och metoder för spridning av styrdokument och relevanta policies naturligt implementeras. Många av bristerna skulle åtgärdas automatiskt om ett ledningssystem för informationssäkerhet implementerades.	Låg

5. Källförteckning

5.1 Kommungemensamma dokument

- Systemförvaltningsmodell Södertälje kommun (2016)
- Informationssäkerhet - instruktioner medarbetare (2016)
- Roller och ansvar for IT och digitalisering i Södertälje kommun (2016)
- Instruktion for informationsklassning (2016)
- Risk och sårbarhetsanalys - Instruktion för IT-system (2016)
- Användarförsäkran (2016)
- Informationssäkerhetspolicy (2014)
- Södertälje kommun Inköpspolicy (2013)
- IT-finansieringsmodell (2011/2012)
- IT-finansieringsmodell - revidering från 160601 (2016)
- Riktlinjer för trådlösa nät (2013)
- Södertälje kommuns riktlinjer för telefoni (2012)
- Inköp av IT-system - riktlinjer upphandling och avtalsförlängning av IT-system (2014)
- e-Södertälje - IT vision och strategi (innan 2009)
- IT-säkerhetspolicy - roller och ansvar för IT-säkerhetsarbetet (2004)
- IT-organisation - roller och ansvar för den generella IT-miljön (2004)
- Riktlinjer för informationssäkerhet (ej antagen ännu)