Building a better working world

Trelleborgs kommun

Rapport: Informationssäkerhetsgranskning
Juli 2021

Sammanfattning

På uppdrag av Trelleborgs kommuns förtroendevalda revisorer har EY genomfört en uppföljande granskning av kommunens arbete med informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende informationssäkerheten, samt följa upp på revisionsgranskningen genomförd 2019.

Följande revisionskriterier användes:

- Myndigheten för samhällsskydd och beredskaps (MBSs) styrningsmodell för offentliga organisationers IT- och informationssäkerhet, LIS.
- ISO/IEC 27000 standarden för informationssäkerhet
- God praxis och EYs erfarenhet inom IT-, Cyber – och informationssäkerhet.

Granskningen genomfördes under april till juni 2021 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad styrdokumentation. Granskningen har byggt på EY:s ramverk för granskning av IT- och informationssäkerhet, Granskningsprogram Cyber och Informationssäkerhet (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 62 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter från kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EYs utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Trelleborgs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en lite högre mognadsgrad, med ett genomsnitt på 2,77 jämfört med jämförelsetalet 2,39. Detta är dock en något lägre mognadsgrad än vad EY rekommenderar för en kommun likt Trelleborgs, givet den stora mängd personuppgifter, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara som högst inom förändringshantering, incidenthantering och nätverk. Lägst anses mognadsgraden inom strategi och rutiner, kontinuitetsplanering och personuppgiftsstyrning.

Kommunens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid. Ett annat förbättringsbehov gäller utbildning inom informationssäkerhet och GDPR, där kommunen rekommenderas att analysera behovet av utbildningar samt säkerställa att dessa erbjuds enligt plan. Iakttagelserna som noterades under granskningen av informationssäkerhet 2019 bedöms delvis åtgärdade. Kommunen har bland annat upprättat centrala rutinbeskrivningar gällande programförändringar och IT-drift men saknar detaljerade rutinbeskrivningar för åtkomsthantering. Vidare har kommunen tillsatt en informationssäkerhetssamordnare och vidareutvecklat den årliga riskanalysen. Detta för att stötta de olika förvaltningarna i att skapa ändamålsenliga rutiner för att uppfylla uppställda krav. Sedan granskningen 2019 har en åtgärdsplan på 96 åtgärder tagits fram. Huruvida alla åtgärder har slutförts i rätt tid eller inte går dock inte att hänvisa från denna plan.

Innehållsförteckning

1. Bakgrund

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

I sin årliga risk- och konsekvensanalys har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet. Dessa risker kan vara kopplade till verksamhetskritiska system inom kommunen. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med IT- och informationssäkerhet. De identifierade riskerna är inte specifikt relaterade till Trelleborgs kommun utan gäller allmänt för stora delar av den offentliga sektorn.

Under 2019 genomfördes en granskning av informationssäkerhet i Trelleborgs kommun. Granskningen identifierade flertalet brister som behövdes åtgärdas och rekommenderade kommunen att ta fram en handlingsplan för detta. Denna granskning avser ge en uppdaterad lägesbild kring hur arbetet med IT- och informationssäkerhet fortskrider.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten utifrån revisionsgranskning genomförd 2019. Vidare är syftet också att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande frågor:

- Har kommunen genomfört de rekommendationer som framkom i informationssäkerhetsgranskningen från 2019?
  - Har kommunstyrelsen vidtagit åtgärder för att göra regelverk kända i organisationen och ta fram detaljerade rutinbeskrivningar för områdena: åtkomst, änderingshantering och drift?
  - Har kommunstyrelsen vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav?
  - Har kommunstyrelsen tagit fram en handlingsplan för att prioritera arbetet utifrån angelägenhetsgrad?

1.2 Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policyer. Granskningen är begränsad till arbetet som Trelleborgs kommun bedriver på central nivå. Intervjuer har endast utförts med representanter på central nivå och inte med representanter i förvaltningarna. Inga bolag har granskats. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

1.3 Metod och genomförande

Granskningen har byggt på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet. Information kring områdena har insamlats både genom granskning av relevanta dokument, samt genom att EY:s specialister genomför granskningsmöten med relevanta personalkategorier i kommunen.

Inledningsvis granskades relevant dokumentation kring kommunens rutiner och processer av EY. Därefter hålls granskningsmöten med kommunens representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av IT- och informationssäkerhet i kommuner. Under granskningen har dock inga stickprovstester utförts, vilket innebär att själva efterlevnaden av kommunens rutiner och kontroller inte testas. Slutligen analyserades och bedömdes den samlade bilden av dokumentation samt information inhämtad via granskningsmöten.

Under granskningen har följande personer intervjuats:

- Stefan Andersson, IT-chef
- Patrik Siltanen, Informationssäkerhetssamordnare
- Malin Ekblad, Säkerhetschef
- Filip Fryklund, Enhetschef IT-drift
- Richard Falk, Projektsamordnare IT

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

Fullständig källförteckning framgår av bilaga 1.

Under uppdraget har EY granskat 5 huvudområden som brutits ner på 18 underområden enligt nedan.

Styrning

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

Personal och behörigheter

- Personal
- Behörighetshantering

Drift

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar

- Förändringshantering

Personuppgifter

- Personuppgiftsstyrning
- Personuppgiftsbehandling
- Personuppgiftsrutiner
- Dataskydd
- Utbildning inom dataskyddsförordningen
- Molntjänster

1.3.1 Bedömning avseende sammanfattande betyg av informationssäkerhetsarbete

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 18 underområden på en skala 1–5. Skalans definition presenteras nedan:

Tabell 1: Skala för bedömning av Trelleborgs Kommuns mognadsgrad inom informationssäkerhetsområden

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

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga delar. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

1.3.1 Tidsplan

Tidsplanen för arbetet såg ut enligt följande:

Förberedelser och planering	April 2021
Insamling och analys av dokumentation	April 2021
Arbetsmöte	April 2021
Rapportskrivning samt intern kvalitetssäkring	Maj 2021
Faktagranskning av kommunen	Juni 2021
Justering samt färdigställande av rapport	Juli 2021
Avrapportering och slutpresentation	Augusti 2021

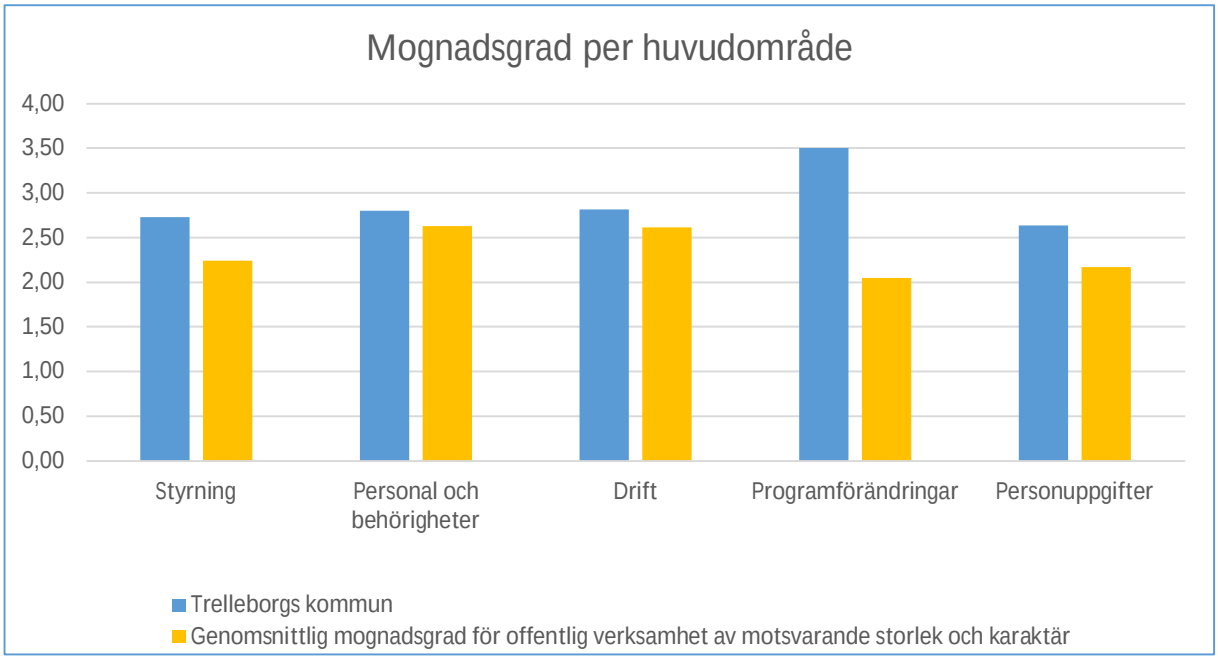
2. Analys

Baserat på den analys och granskning som genomförts bedöms Trelleborgs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en lite högre mognadsgrad, med ett genomsnitt på 2,77 jämfört med jämförelsetalet 2,39. Detta är dock en något lägre mognadsgrad än vad EY rekommenderar för en kommun likt Trelleborgs, givet den stora mängd personuppgifter, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara som högst inom förändringshantering, incidenthantering och nätverk. Lägst anses mognadsgraden inom strategi och rutiner, kontinuitetsplanering och personuppgiftsstyrning.

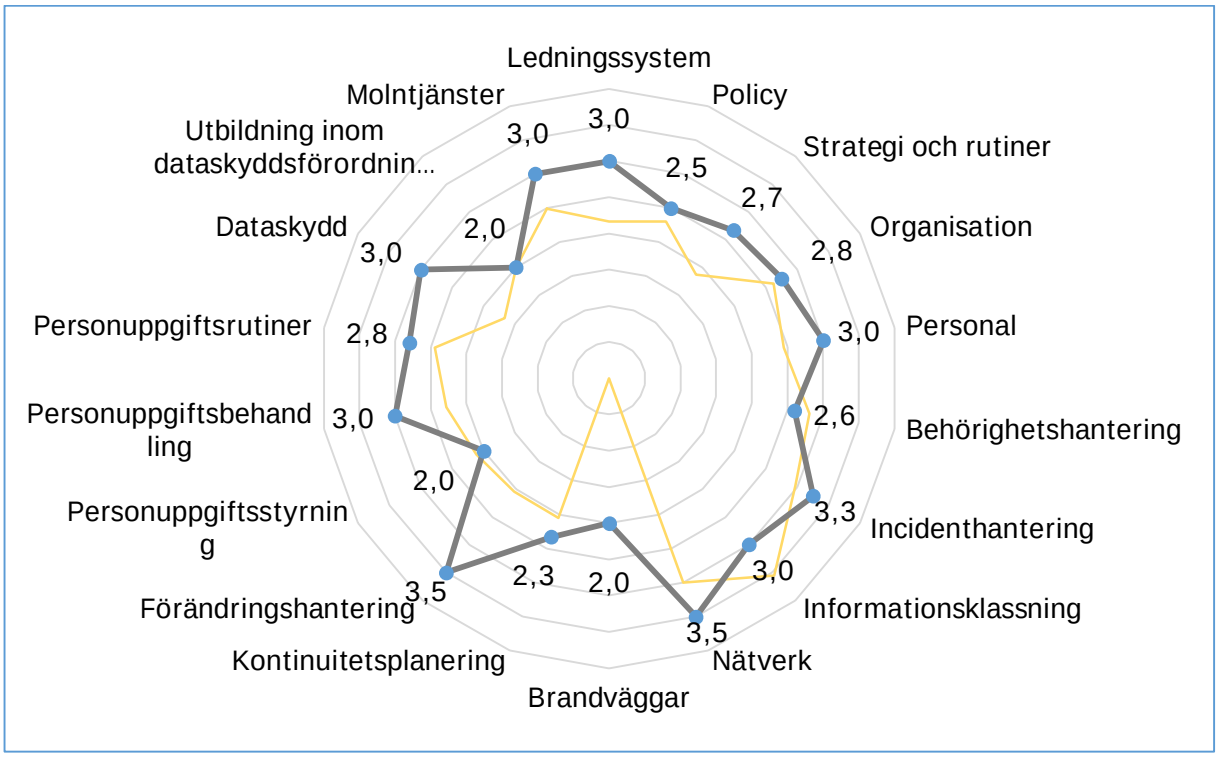
Kommunen har upprättat relevanta och omfattande styrdokument med tillhörande riktlinjer och en tydlig ansvarsfördelning kring arbetet med informationssäkerhet inom kommunen. Det har även påvisats att flertalet åtgärder tagits sedan informationssäkerhetsgranskningen som genomfördes under 2019. Kommunens personal uppvisar även stor kunskap inom informationssäkerhetsområdet samt ambitioner om att fortsätta utveckla arbetet inom området.

Kommunens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid. Ett annat förbättringsbehov gäller utbildning inom informationssäkerhet och GDPR, där kommunen rekommenderas att analysera behovet av utbildningar samt säkerställa att dessa erbjuds enligt plan.

Bilden nedan (Figur 1) redovisar kommunens mognadsgrad för de 5 huvudområden som granskats, samt nedbrutet på 18 underområden (Figur 2).



Figur 1 – Överblick över kommunens mognadsgrad för de fem huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär (gula staplar).



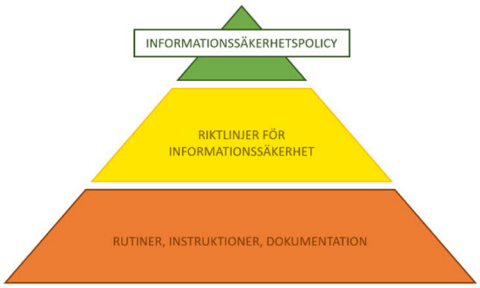
Figur 2 – Överblick över kommunens mognadsgrad för de fem huvudområden som granskats nedbrutet på 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär (gul linje).

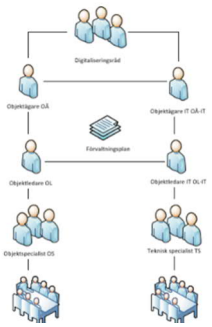
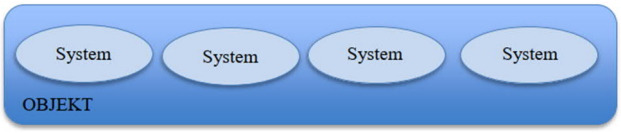
2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se Tabell 2).

Tabell 2: Nuläge och iakttagelser inom huvudområdet Styrning

Område	Nuläge	Iakttagelser	Mognad
Lednings-system	Trelleborgs kommun har enligt styrande dokument etablerat ett Ledningssystem för informationssäkerhet (LIS) baserat på ISO/IEC 27001, *Ledningssystem för informationssäkerhet* och ISO/IEC 27005 - *Riskhantering*. Ledningssystemet innebär att informationssäkerhetsarbetet ska ske på ett systematiskt och standardiserat sätt, där Trelleborgs kommun och bolag följer ett årshjul för att planera, följa upp och utvärdera informationssäkerhetsarbetet. Ledningssystemet innebär att kommunen har en policy för informationssäkerhet med kompletterande riktlinjer, samt att Trelleborgs kommuns medarbetare ska få utbildning i informationssäkerhet årligen. Vidare ska informationssäkerhetssamordnaren årligen sammanställa en rapport över hur arbetet med informationssäkerhet pågår inom Kommunen. Rapporten ska därefter distribueras till kommunstyrelsen och de nämnder som är egna vårdgivare.	-	3,0

Policy	Trelleborgs kommuns arbete med informationssäkerhet beskrivs på en övergripande nivå i den nuvarande informationssäkerhetspolicyn som fastslogs 2018. I *Informationssäkerhetspolicyn* fastställs Trelleborgs kommuns syn på informationssäkerhet samt övergripande mål och roller. Informationssäkerhetspolicyn fungerar således som det överordnade och styrande dokumentet. I *Riktlinjer för informationssäkerhet* beskrivs vilka rutiner och säkerhetslösningar som måste etableras för att uppfylla de mål som beskrivs i *Informationssäkerhetspolicyn* (se Figur 3). Riktlinjerna berör huvudområdena inom IT- och informationssäkerhet såsom lösenord och autentisering, behörighets-, förändrings- och incidenthantering. Vidare har även kommunen tillsett ett antal rutiner och instruktioner för hur informationssäkerhetsarbetet ska bedrivas såsom mallar för riskanalys. Riktlinjerna syftar till att etablera en gemensam säkerhetsnivå som kommunens olika delar minst förväntas uppfylla. Medarbetare kan nå dokumenten via kommunens intranät.  *Figur 3 - Schematisk överblick över strukturen av styrdokumenten i Trelleborgs kommun* Enligt Trelleborgs kommuns *Riktlinjer för informationssäkerhet* ska policyn revideras var tredje år och riktlinjer ses över och uppdateras löpande, eller åtminstone var tredje år i samband med uppdateringen av *Informationssäkerhetspolicyn*.	Informationssäkerhetspolicyn samt tillhörande riktlinjer granskas och uppdateras med en för låg frekvens för att förbli aktuella.	2,5
Strategi och rutiner	Det finns en enhet inom kommunstyrelsen som arbetar med digital utveckling, digitaliseringsrådet, som har utformat en digital agenda innehållande övergripande IT-mål etc., gemensam för samtliga förvaltningar inom kommunen. Med utgångspunkt i den digitala agendan utvecklar respektive förvaltning digitaliseringsplaner innehållande kort- och långsiktiga mål för IT. Den digitala agendan har dock ej uppdaterats sedan 2018. Kommunen har definierat en övergripande anvisning för användningen av kommunens IT-miljö som gäller för alla användare i kommunens olika verksamheter. I denna övergripande anvisning *riktlinjer för informationssäkerhet* beskrivs regler och riktlinjer för hur medarbetare ska använda kommunens datorer och andra digitala enheter, internet, e-post och lösenord.	Kommunens digitala agenda som definierar riktningen för IT har inte uppdaterats sedan 2018.	2,7

	Kommunen har även upprättat en central rutinbeskrivning för programförändringsprocessen och delvis för drift. Det är därefter upp till systemägare att upprätta separata rutinbeskrivningar för respektive IT-system.		
Organisation	Organisationen och dess ansvar för Trelleborgs kommuns informationssäkerhetsarbete stipuleras i kommunens informationssäkerhetspolicy, Riktlinjer för informationssäkerhet samt digitaliserings- och systemförvaltningsmodellen. Kommunens säkerhetschef är ägare av informationssäkerhetspolicyn som fastställs av kommunstyrelsen. Det är denna policy som styr kommunens arbete med informationssäkerhet. I policyn beskrivs även de olika ansvarsområden inom detta arbete. Även kommunens förvaltningsmodell för IT beskriver roller som är relevanta från ett informationssäkerhets-perspektiv. Förvaltningsmodellen IT upprättades 2018 (uppdaterad senast 2019-04-12) och stipulerar att alla kommunens system ska organiseras i så kallade förvaltningsobjekt med en styrgrupp och en förvaltningsgrupp där systemen ingår (se Figur 4, 5 & 6).  *Figur 4: Illustration över Trelleborgs kommuns förvaltningsmodell (1)*  *Figur 5: Illustration över Trelleborgs kommuns förvaltningsmodell (2)*  *Figur 4: Illustration över hur systemen är organiserade i förvaltningsobjekt* Vid upphandlingar av informationssystem och hantering av leverantörsavtal läggs stort ansvar på systemägare och systemförvaltare. Inför upphandling av informationssystem finns det dokumenterade krav på att en riskanalys ska genomföras. Det är den potentiella systemägarens ansvar att riskanalysen genomförs, men informationssäkerhetssamordnaren kan vara involverad om behovet finns. Upphandlingen ska ske i samråd med IT-avdelningen. Metoden för att		2,8

	genomföra riskanalyser finns dokumenterad i *Riktlinjer för informationssäkerhet.* I dokumentet *Riktlinjer för informationssäkerhet* framgår att systemägaren och systemförvaltare för respektive system ansvarar för att följa upp att relevanta avtal (SLA) finns med leverantörer och att dessa efterlevs. Hur uppföljningen ska genomföras samt vilka krav som ska uppfyllas för att säkerställa att säker informationshantering efterlevs finns däremot inte dokumenterat. Under intervjuer med nyckelpersoner framkom det att uppföljningen görs som del av den årliga riskanalysen där avsnitten som berör leverantören, såsom exempelvis drift och säkerhet, skickas ut till och besvaras av leverantören inför riskanalysen. Systemägaren bär ansvaret för att svaren samlas in. Slutligen granskas svaren och leverantörens efterlevnad av IT och informationssäkerhetssamordnaren.	Trelleborgs kommun saknar en dokumenterad processbeskrivning över hur uppföljning av leverantörer ska genomföras samt vilka krav som ska uppfyllas för att säkerställa att säker informationshantering efterlevs.	

2.2 Personal och behörigheter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personal och behörigheter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område	Nuläge	Iakttagelser	Mognad
Personal	Trelleborgs kommun har sedan 2017 en tillsatt informationssäkerhetssamordnare som arbetar på halvtid. Samordnaren arbetar dedikerat med frågor rörande informationssäkerhet. Under den då rådande pandemin har medarbetare inom Trelleborgs kommun arbetat med kompetensutveckling av nyckelpersonal inom informationssäkerhet. Detta med syftet att minska personberoendet inom kommunens arbete. I mars 2021 utvecklades en pandemiplan där kommunens kompetens- och resursbehov för att kunna bedriva verksamheten sågs över. Enligt intervjuade nyckelpersoner ska samtliga medarbetare inom kommunen erbjudas utbildning inom informationssäkerhet och GDPR årligen. Trelleborgs kommun använder sig av så kallade nano-learnings, korta utbildningssekvenser på ca fem minuter med olika fokusområden. Under 2019 valde Trelleborgs kommun att fokusera nano-learnings på området GDPR och under våren 2021 på informationssäkerhet. Målsättningen med nano-learnings är att bidra med generell kunskapshöjning inom dataskydd och informationssäkerhet till anställda. Resultat och statistik över deltagande följs	Kommunen har ej genomfört planlagda och årliga utbildningsinsatser inom informationssäkerhet.	3,0

	upp av informationssäkerhetssamordnaren en vecka efter genomförd utbildning. Implementeringsarbetet med nano-learnings fortgår enligt intervjuade nyckelpersoner.		
Behörighets-hantering	Medarbetarens anställning styr om medarbetaren ska ha ett Active Directory (AD)-konto eller inte. Enligt styrande dokument ska samtliga användarkonton vara personliga för de system som hanterar information som klassificeras som nivå 1 eller högre. För IT-avdelningen innebär det att alla har dubbla konton, ett användarkonto och ett med högre behörighet för administration. Systemadministratörer/tekniker ska alltid ha individuella behörigheter. Om det inte är möjligt med individuella behörigheter ska det föras en manuell logg över vem som använt ett gruppkonto. För system synkroniserade med AD är närmaste chef vid nyanställning ansvarig för att skicka en beställning av nytt användarkonto till HR. HR-avdelningen ansvarar därefter för att skapa kontot i HR-systemet. När användaren är registrerad i HR-systemet kan ett AD-konto sättas upp tidigast 30 dagar innan påbörjad anställning. AD-konton inaktiveras per automatik under den anställdes registrerade sista anställningsdag i HR-systemet. Det är närmaste chef som är ansvarig för att meddela HR om den anställdes sista arbetsdag. För verksamhetssystem och övriga system som inte är AD-synkroniserade finns det inga generella riktlinjer utan det är förvaltningarna som är ansvariga för att sätta upp egna rutiner och processer för behörighetshanteringen. Systemägaren ansvarar för att personerna som finns i systemet har rätt behörighet. Det genomförs inte en central periodisk genomgång av behörigheter i kommunens system utan det ansvarar varje verksamhetssystems systemägare för. Enligt de interna riktlinjerna ska detta genomföras i samband med den årliga genomgången av riskanalysen. Dock finns det ingen gemensam instruktion för hur detta ska genomföras eller vilka krav som behöver uppfyllas. Systemägaren ansvarar även för att ta fram användarrutiner för behörighetshantering. Trelleborgs kommuns *riktlinjer för informationssäkerhet* innehåller lösenordspolicy med följande krav: - Minst 12 tecken - Inte samma som de senaste 30 lösenorden - Inte återanvända samma lösenord inom 1 år - Bytas minst var 90e dag - Innehålla versaler och specialtecken	Trelleborgs kommun har ingen centralt definierad och dokumenterad behörighetsprocess för nytilldelning, förändring och avslutning av användarbehörigheter till kommunens informationssystem.	2,6

2.3 Drift

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *drift* samt de iakttagelser som noterats under granskningens utförande (se Tabell 4).

Tabell 4: Nuläge och iakttagelser inom huvudområdet Drift

Område	Nuläge	Iakttagelser	Mognad
Incident-hantering	Inom Trelleborgs kommun delas säkerhetsincidenter in i tre kategorier; NIS-säkerhetsincidenter, IT-säkerhetsincidenter och personuppgiftsincidenter (se kapitel 2.5). Hantering av informationssäkerhetsincidenter beskrivs i kommunens *Riktlinjer för informationssäkerhet* samt *Rutiner för IT säkerhetsincidentrapportering* och *Rutiner för NIS säkerhetsincidentrapportering*. I de inköpta informationssystemen ansvarar leverantören för övervakning och kontroll av den tekniska driftmiljön och ska logga incidenter orsakade av tekniska brister och externa störningar. Enligt rutinerna ska säkerhetsincidenter, eller misstänkta säkerhetsincidenter, som kan påverka informationssäkerheten omgående rapporteras till närmaste chef som tar ärendet vidare med IT-avdelningen, DSO och berörda parter. Incidenter som anses vara kritiska ska enligt rutinerna eskaleras omgående till beställaren (IT-avdelningen) och vid kvartalsvisa uppföljningar (säkerhetsforum) ska leverantören redovisa alla inträffade incidenter, typer och statistik samt analyser av sårbarheter. Enligt rutinerna har anställda, uppdragstagare och tredjepartsanvändare av informationssystem och tjänster även som ansvar att notera och rapportera observerade eller misstänkta säkerhetsbrister i system eller tjänster. Incidenter och säkerhetsmässiga svagheter ska i dessa fall rapporteras omgående till systemägare och informationssäkerhetsansvarig. Servicedesk fungerar som en kontaktpunkt som anställda kan använda för att göra felanmälningar och rapportera incidenter.		3,3
Informations-klassning	Trelleborgs kommun har enligt intervjuade nyckelpersoner genomfört en informationsklassificering av samtliga informationssystem under 2021 baserad på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Utifrån informationsklassificeringen får systemet ett skyddsvärde mellan 0-3 för respektive informationssäkerhetsprincip, som därefter styr rekommendationerna för lämpliga säkerhetsåtgärder för bl.a. åtkomst, loggning, säkerhetskopiering, anskaffning/utveckling av system, leverantörer, drift etc.	-	3,0

	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. Det är systemägaren för respektive system som ansvarar för att informationsklassningen genomförs. Riskanalyser ska enligt *riktlinjer för informationssäkerhet* ske på system inom kommunen som hanterar information som klassificeras som nivå 1 eller högre. För mindre system som hanterar information lägre än nivå 1, eller nivå 1 och i väldigt liten omfattning, behöver endast en grundläggande genomgång för IT- och informationssäkerhet genomföras. Det är IT-avdelningen och informationssäkerhetssamordnaren som bedömer huruvida en riskanalys behöver genomföras eller inte. Det är systemägare för respektive system som ansvarar för att riskanalysen har genomförts. Trelleborgs kommun har tagit fram mallar för hur riskanalysen ska genomföras, både för mindre kritiska och kritiska system.		
Nätverk	Enligt intervjuade nyckelpersoner har Trelleborgs kommun segregerat informationssystemen både logiskt och fysiskt fysisks i enlighet med kraven från NIS. De ska även ha implementerat ”intrusion detection system” (IDS) och ”intrusion prevention system” (IPS) för att analysera nätverksaktiviteter.	-	3,5
Brandväggar	Enligt Trelleborgs kommun granskar de brandväggarnas konfiguration på månadsbasis. Vidare sker samtliga förändringar i brandväggarnas konfiguration enligt processen för programförändringar, vilken beskrivs i kapitel 2.4 nedan. Kommunen har däremot för nuvarande ingen dokumenterad brandväggspolicy för att styra underhåll och dokumentation av brandväggsrelaterade aktiviteter.	Trelleborgs kommun har ingen brandväggspolicy eller dokumenterade rutiner för att på regelbunden basis granska och testa brandväggarnas konfiguration.	2,0
Kontinuitetsplanering	Kommunen har en centralt utarbetad policy med tillhörande riktlinjer för kris och verksamhetskontinuitet. Under intervju med nyckelpersoner framkom det att det genomförs risk och sårbarhetsanalyser för samhällsviktiga tjänster (NIS) och att varje verksamhet har en egen kontinuitets- eller krisplan. I verksamheternas kontinuitetsplaner bedöms kritiska beroenden och planer för hur verksamheten ska bedrivas vid inträffandet av en kris eller katastrof och avsaknad av kritiska funktioner såsom informationstillgångar, IT-system, samt hur återställningen till normalläge ska ske. Då ansvaret för kontinuitetsarbetet ligger på verksamhetsnivå finns inga centrala kontinuitetsplaner för verksamhetsgemensamma system. Kommunen saknar i dagsläget en kategorisering av IT-systemen	IT behandlas inte tillräckligt i Kommunens kontinuitetsarbete, exempelvis saknas verksamhetsövergripande planer för kritiska IT-system samt en prioriterad plan för återställande av system.	2,3

	utifrån dess kritikalitet samt en tydlig koppling mellan kritikalitet och vikt i kontinuitetsarbetet. Det saknas i dagsläget exempelvis en prioriteringsordning i vilken systemen ska återställas efter en kris.		

2.4 Programförändringar

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *programförändringar* samt de iakttagelser som noterats under granskningens utförande (se Tabell 5).

Tabell 5: Nuläge och iakttagelser inom huvudområdet Programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Kommunen har en definierad programförändringsprocess för hur IT-avdelningen i Trelleborgs kommun ska arbeta med att registrera och behandla behov och önskemål om förändringar i kommunens IT-tjänster samt genomföra och utvärdera förändringar i kommunens IT-tjänster. Enligt denna process delas programförändringar in i tre typer: standard-, normal- och krisförändringar. Change managern granskar därefter förändringsförfrågningar, ”request for change” (RFC), och utvärderar exempelvis förändringens orsak, nytta och risk. Detta resulterar i tre kategorier av förändringar; mindre, signifikant och större förändring. Förändringar av typen standard kräver endast godkännande av enskild medarbetare på IT-avdelningen, normal av omfattningen mindre förändring av change managern, normal-förändring av omfattningen signifikant eller större kräver godkännande av CAB (Change Advisory Board) och krisförändring kräver godkännande av IT-chef i samband med change manager. CAB består av change manager (sammankallande), IT-chef samt IT- och verksamhetsrepresentanter efter behov. Patchningar från externa leverantörer sker utifrån prioritet och kategorisering av spårbarhet.	-	3,5

2.5 Personuppgifter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personuppgifter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 6).

Tabell 6: Nuläge och iakttagelser inom huvudområdet Personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts-styrning	Trelleborgs kommun har en dokumenterad instruktion för hantering av GDPR i Trelleborgs digitala kanaler. Kommunen har även tagit fram diverse andra rutiner och instruktioner rörande hanteringen av	Kommunens saknar styrande dokument gällande personuppgiftsstyrning.	2,0

	personuppgifter. Dessa dokument finns tillgängliga på Trelleborgs intranät. Vad som ligger bakom namngivningen av respektive dokument är dock oklart, där skillnaden på instruktioner, riktlinjer, beskrivning och rutiner ej framgår. Varje förvaltning ska ha en utsedd representant som ansvarar för arbetet med personuppgifter. En gång per kvartal ska alla representanter samlas och diskuterar vad som behöver göras inom GDPR och distribuerar uppgifter baserat på det som diskuterats. Mötesanteckningar ska därefter publiceras på kommunens intranät.	Kommunen har en delvis ostrukturerad dokumenthantering relaterade till personuppgifter.	
Personuppgifts-behandling	Trelleborgs kommun använder sig av ett systemstöd för att upprätthålla en registerförteckning för behandling av personuppgifter. Detta register avser att uppfylla artikel 30 i dataskyddsförordningen och beskriver exempelvis vilka kategorier av personliga data som kommunen hanterar. Kommunens dataskyddsombud (DSO) har ansvar för att säkerställa att respektive nämnds område behandlar personuppgifter på ett korrekt och lagligt sätt och är även kontaktperson i relation till Integritetsskyddsmyndigheten (IMY). För behandlingar som utförs av andra parter ska personuppgiftsbiträdesavtal (PUB-avtal) tecknas med dessa leverantörer. Efterlevnadskontroll av leverantörer ska skötas av kommunens DSO som även ska säkerställa att alla PUB-avtal hålls uppdaterade över tid.	Kommunen saknar en dokumenterad rutin för att följa upp och säkerställa att registerförteckningar i systemstödet är uppdaterade och kompletta över tid.	3,0
Personuppgifts-rutiner	Kommunen har en definierad process för hantering av personuppgiftsincidenter. Incidenter kopplade till personuppgifter ska rapporteras till förvaltningarnas respektive GDPR-samordnare, som tillsammans med kommunens DSO, närmaste chef och medarbetaren som anmält incidenten ska besluta om incidenten ska rapporteras eller inte samt vilka åtgärder som behöver vidtas. GDPR-samordnarna är därefter ansvariga för att vidta de åtgärder som behövs och rapportering till IMY, dokumentation samt information till registrerade. Processen beskrivs i Trelleborgs kommuns *rutiner för personuppgiftsincident*. Kommunen har även tagit fram en checklista för hantering av personuppgiftsincidenter som finns i *Process checklista personuppgiftsincidenter hos personuppgiftsansvariga*. Det finns en definierad process för att svara på förfrågningar från registrerade angående begäran om registerutdrag, detta beskrivs i *Rutiner för begäran om registerutdrag*. Förfrågningarna ska enligt denna process alltid hanteras via kundtjänst som tar vidare ärendet till ansvarig förvaltning. Kommunen har även skapat *mall för registerutdrag*, *riktlinjer information till*	Det saknas en rutin för hantering av inkommande begäran från registrerade gällande rättelse, begränsning eller radering av personuppgifter.	2,8

	registrerad med mall, *riktlinje kring hantering av personuppgifter* och *riktlinje e-post*. Det saknas däremot en definierad process för rättelse, begränsning och radering av personuppgifter på begäran av registrerade. Kommunen har tagit fram rutiner för gallring och lagring av personuppgifter i *riktlinjer med dataskyddsförordningen i Trelleborgs kommuns digitala kanaler* samt *Arkivlagen och GDPR.* Kommunen genomför ingen uppföljning av förvaltningarnas efterlevnad utan lägger det på respektive förvaltning.	Det finns ingen dokumenterad process för kontinuerlig granskning gällande efterlevnaden av rutiner och instruktioner kopplade till personuppgiftshanteringen inom kommunen.	
Dataskydd	Kommunen arbetar enligt intervjuade nyckelpersoner strukturerat med dataskydd och har tekniska åtgärder inbyggda i IT-systemen som används för att leva upp till kraven på databehandling. Dataskydd ska även vara en parameter som bedöms vid upphandling av nya system.	-	3,0
Utbildning inom dataskydds-förordningen	Enligt Trelleborgs kommuns utbildningsplan ska samtliga anställda inom kommunen årligen genomföra korta utbildningssekvenser, s.k. nano-learnings inom GDPR. Resultat och statistik över deltagande följs upp av informationssäkerhetssamordnaren en vecka efter genomförd utbildning.	Inga utbildningsinsatser inom GDPR har genomförts under 2020 eller 2021. Den senast genomförda utbildningen inom GDPR var år 2019.	2,0
Molntjänster	Kommunen uppger att man har avsikt att följa SKR:s vägledning och riktlinjer för personuppgifter hanterade i molntjänster, speciellt framtagna för att vägleda och hjälpa kommuner och regioner analysera frågor om juridik och säkerhet för molntjänster.	-	3,0

3. Övergripande rekommendationer

Iakttagelser av varierande vikt har identifierats inom flera delar av ramverket. EY har därför valt att presentera de mest relevanta övergripande rekommendationerna för Trelleborgs kommun och förslag på åtgärder för de främsta riskerna inom informationssäkerhetsarbetet. EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Styrdokument

Bland Trelleborgs kommuns styrdokument finns en informationssäkerhetspolicy med tillhörande riktlinjer samt en digital agenda gemensam för förvaltningarna inom kommunen. Kommunen har en ambition om att genomföra en genomgång av policyn var tredje år och uppdatering av riktlinjer löpande. Vidare finns ambitioner om en årlig uppdatering av den digitala agendan, men styrdokumentet har ej uppdaterats sedan 2018. EY bedömer att styrande dokument granskas och uppdateras med för låg frekvens. Brist på regelbunden uppdatering av policydokumentation medför en risk att arbetet med informationssäkerhet fortskrider utan grund i övergripande beslut och utifrån utdaterade och irrelevanta metoder, vilket kan leda till att riktighet, spårbarhet, konfidentialitet och tillgänglighet av informationen som hanteras ej säkerställs. EY rekommenderar att kommunen tillser att styrande dokument uppdateras i enlighet med säkerhetsbehovet eller minst årligen, för att reflektera organisations nuvarande behov samt omvärldens förändringar och krav.

Utbildning inom IT- och informationssäkerhet

Enligt intervjuade nyckelpersoner ska samtliga medarbetare inom kommunen erbjudas utbildning inom informationssäkerhet och GDPR årligen. EY noterade dock under granskningen att utbildningarna inte erbjudits enligt plan, då exempelvis inga utbildningsinsatser gällande GDPR har genomförts sedan 2019. Kommunen rekommenderas att analysera behovet av utbildningar och dess effekt på kunskapsnivån hos medarbetare och anpassa utbildningsinsatserna därefter. Vidare rekommenderas kommunen säkerställa att utbildningarna erbjuds enligt plan.

Rutin för behörighetshantering

Efter granskningen av informationssäkerhet som genomfördes under 2019 har rutiner för IT-drift och programförändringsprocessen upprättats. Det saknas däremot övergripande riktlinjer på central nivå för behörighethantering, såsom processen för tilldelning, förändring och borttag av behörighet, samt periodiska genomgångar av behörigheter. EY rekommenderar kommunen att upprätta operationella rutiner för processerna inom behörighetshanteringen.

Kontinuitetsplanering

Kommunen genomför risk och sårbarhetsanalyser för samhällsviktiga tjänster (exempelvis enligt NIS-direktivet) där varje verksamhet har en egen kontinuitets- och krisplan. Verksamheternas kontinuitets- och krisplaner behandlar endast IT som ett av många delområden. För att minska sårbarheten vid eventuella störningar eller avbrott rekommenderar EY därmed Trelleborgs kommun att göra en bedömning av IT-systems kritikalitet för verksamheterna samt länka detta till arbetet med kontinuitets- och krisplaner. Exempelvis bör beroenden mellan system klargöras, samt i vilken ordning de

ska återställas efter en kris. Vidare bör de mest kritiska systemen få en större del i kontinuitetsplaneringen då de kan få stor effekt vid eventuell kris och påverka många separata verksamheter.

4. Revisionsfrågor

Granskningen har utgått från fyra revisionsfrågor, vilka besvaras nedan.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Har kommunen genomfört de rekommendationer som framkom i informationssäkerhetsgranskningen från 2019?	Trelleborgs kommun har påbörjat arbetet för att åtgärda de brister som noterades under informationssäkerhetsgranskning 2019. Se nedan revisionsfrågor för bedömningar om genomförandet för respektive rekommendation.	
▸ Har kommunstyrelsen vidtagit åtgärder för att göra regelverk kända i organisationen och ta fram detaljerade rutinbeskrivningar för områdena: åtkomst, änderingshantering och drift?	Kommunstyrelsen har delvis vidtagit åtgärder för att göra regelverk kända i organisationen och delvis tagit fram detaljerade rutinbeskrivningar för områdena: åtkomst, ändringshantering och drift. Kommunen har bland annat tagit fram rutinbeskrivningar över hur kommunens IT-avdelning arbetar med att registrera och behandla behov och önskemål om förändringar, samt genomför och utvärderar förändringar, i kommunens IT-tjänster. Vidare har kommunstyrelsen tagit fram beskrivningar kring infrastrukturen och systemdrift för IT. Det saknas däremot detaljerade rutinbeskrivningar för åtkomsthantering. Beskrivningarna gäller kommunens centrala IT-system och det är upp till respektive systemägare att sätta upp rutiner för egna IT-system. Stickprover på enskilda system har inte genomförts som en del av denna granskning. Kommunen har även påbörjat utbildningsinsatser i form av nano-learnings inom områdena GDPR och informationssäkerhet för att göra regelverk kända i organisationen.	

	Implementeringsarbetet fortgår, vilket varit ett bidrag till att punkten bedöms vara delvis åtgärdad.	
► Har kommunstyrelsen vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav?	Kommunstyrelsen bedöms ha vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav. Kommunstyrelsen har sedan 2019 års granskning tillsatt en informationssäkerhetssamordnare på halvtid för att driva dessa frågor. Vidare har kommunstyrelsen sedan 2019 års granskning vidareutvecklat den årliga uppföljande riskanalysen till en större omfattning för att stötta de olika förvaltningarna i att skapa ändamålsenliga rutiner för att uppfylla uppställda krav. Riskanalysen omfattar bl.a. sekretess, riskregister, skyddsåtgärder och säkerhetskopiering. Vid genomgången kan de olika förvaltningarna få stöd från informationssäkerhetssamordnaren.	
► Har kommunstyrelsen tagit fram en handlingsplan för att prioritera arbetet utifrån angelägenhetsgrad?	Trelleborgs kommun har delvis tagit fram en handlingsplan för att prioritera arbetet utifrån angelägenhetsgrad. En handlingsplan på 96 punkter uppdelat på de fyra systemen som granskningen 2019 omfattade togs fram efter granskningen. Handlingsplanen anger identifierad brist, ansvarig person och deadline för respektive åtgärd. Enligt intervjuade nyckelpersoner har samtliga 96 identifierade brister blivit åtgärdade, men eftersom ingen prioritering av arbetet mellan de olika åtgärderna gjorts, det saknas spårbarhet i handlingsplanen i form av status för åtgärderna samt att de utsatta deadlines för åtgärderna inte hållits anses denna revisionsfråga endast delvis uppfylld.	

5. Slutsatser

Granskningens syfte har varit att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten utifrån revisionsgranskning genomförd 2019. Vidare är syftet också att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp arbetet på området. Syftet har besvarats med hjälp av följande frågor:

- Har kommunen genomfört de rekommendationer som framkom i informationssäkerhetsgranskningen från 2019?
  - Har kommunstyrelsen vidtagit åtgärder för att göra regelverk kända i organisationen och ta fram detaljerade rutinbeskrivningar för områdena: åtkomst, änderingshantering och drift?
  - Har kommunstyrelsen vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav?
  - Har kommunstyrelsen tagit fram en handlingsplan för att prioritera arbetet utifrån angelägenhetsgrad?

Baserat på den analys och granskning som genomförts bedöms Trelleborgs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en lite högre mognadsgrad, med ett genomsnitt på 2,77 jämfört med jämförelsetalet 2,39, på en femgradig skala. Mognadsgraden bedöms vara som högst inom förändringshantering, incidenthantering och nätverk. Lägst anses mognadsgraden inom strategi och rutiner, kontinuitetsplanering och personuppgiftsstyrning. EY rekommenderar dock kommuner att sträva efter en högre mognadsgrad än vad Trelleborgs kommun i dagsläget uppnår.

Kommunens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid. Ett annat förbättringsbehov gäller utbildning inom informationssäkerhet och GDPR, där kommunen rekommenderas att analysera behovet av utbildningar samt säkerställa att dessa erbjuds enligt plan.

Iakttagelserna som noterades under granskningen av informationssäkerhet 2019 bedöms delvis åtgärdade. Kommunen har bland annat upprättat centrala rutinbeskrivningar gällande programförändringar och IT-drift men saknar detaljerade rutinbeskrivningar för åtkomsthantering. Vidare har kommunen tillsatt en informationssäkerhetssamordnare och vidareutvecklat den årliga riskanalysen för att stötta de olika förvaltningarna i att skapa ändamålsenliga rutiner för att uppfylla uppställda krav. Sedan granskningen 2019 har en åtgärdsplan på 96 åtgärder tagits fram och samtliga punkter har enligt intervjuer med nyckelpersonen åtgärdats. EY rekommenderar att kommunen arbetar vidare med åtgärdsplanen och verifiera att samtliga punkter åtgärdats, samt upprättat centrala operationella rutiner för behörighetshantering för att säkerställa att rekommendationerna från informationssäkerhetsgranskningen 2019 vidtagits.

Bilaga 1: Källförteckning

Intervjuade roller:

- Malin Ekblad, Säkerhetschef *2021-04-26*
- Stefan Andersson, IT-chef *2021-04-26*
- Patrik Siltanen, Informationssäkerhetssamordnare & DSO *2021-04-26*
- Filip Fryklund, Enhetschef IT-drift *2021-04-26*
- Rickard Falk, Projektsamordnare IT *2021-04-26*

Dokumentförteckning:

- Arbetmarknad PUA-PUB
- Behandling av personuppgifer på Slättnet
- Bildningsnämnden PUA-PUB
- Fredrik Magnusson – Trelleborg Energiförsäljning AB
- Fritidsnämnden och Kultur & Fritid PUA-PUB
- Information om överföring till USA
- Kommunstyrelsen och Kommunövergripande behandlingar PUA-PUB
- Personuppgifter – Trelleborg
- Samhällsbyggnad PUA-PUB
- Socialnämnden PUA-PUB
- Tekniska servicenämnden PUA-PUB
- Trelleborg Elnät AB
- Trelleborg Hamn AB
- Trelleborg Hem PUA-PUB
- Trelleborgs Energiförsäljning PUA-PUB
- Trelleborgs Fjärrvärme AB
- Valnämnden PUA-PUB
- Visit Trelleborg
- Överförmyndarnämnden PUA-PUB
- Informationssäkerhet vid hantering av mindre IT-system LIS
- Formulär – Begäran om registerutdrag Trelleborg
- Mall för registerutdrag
- Registerutdrag – PUA Trelleborg
- Registrera personuppgiftsbehandling & Begäran inlogg
- Riktlinje för informationssäkerhet
- Rutin för begäran om registerutdrag Trelleborg
- Trelleborg.se_personuppgifter på plats
- Arkivlagen och GDPR
- Beskrivning logg personuppgiftsincidenter
- Blankett anmälan av personuppgiftsincident
- Checklista IT och informationssäkerhet vid hantering av mindre IT-system
- Formulär för säkerhetsincident
- GDPR incidentlogg håll ordning och reda
- Instruktioner samtyckesblankett
- Mall för den personuppgiftsansvariges Instruktion för behandling av personuppgifter
- Mall underbiträden
- Modellavtal Trelleborgs kommun
- Personuppgiftsbiträdesavtal

- Personuppgiftsincident
- Process checklista personuppgiftsincidenter hos personuppgiftsansvariga
- Resurser personuppgifter – information till medborgaren via kommunens hemsida
- Resurser
- Riktlinje kring hantering av personuppgifter
- Riktlinje e-post
- Riktlinjer 20180411
- Riktlinjer information till registrerad – medmall
- Riktlinjer konsekvensbedömning
- Samtycke publicering personuppgifter Trelleborg 1 person
- Bilaga 2, Formulär för säkerhetsincidentrapportering
- Bilaga 3, Formulär för riskanalys av mindre IT-system
- Bilaga 4, Rutin för IT säkerhetsincidentrapportering
- Bilaga 5, Rutin för NIS säkerhetsincidentrapportering
- Bilaga 6, Formulär kontaktuppgifter
- Bilaga 7, Avtal avseende autentisering av personer
- Bilaga 8a NIS-direktivet – Riskanalys för informationssäkerhet
- Bilaga 8b NIS-direktivet – samhällsviktiga och digitala tjänster
- Bilaga 14, Rutin hemarbete
- Bilaga 15, Gallring och bevarande av e-post
- Change-processen
- Digital agenda Trelleborg
- Handlingsplan revision
- Incidentprocessen
- IT-drift Infrastruktur
- IT-drift Systemdrift
- Policy informationssäkerhet
- RFC Jedox
- Riktlinje för informationssäkerhet
- Riktlinjer för informationssäkerhet – *Uppdaterad 2021*
- Styrdokument förvaltningsmodell objekt 190423
- Systemdokumentation

Bilaga 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.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Backup: Säkerhetskopia av den information som finns i en databas eller på en server.

CAB (Change Advisory Board): Styrgrupp för att fatta beslut kring hantering av programförändringar och utveckling av verksamhetens informationssystem.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

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.

Förvaltningsobjekt: Styrande enhet inom vilken ett antal olika informationssystem för en viss typ av kommunens verksamhet innefattas. Förvaltningsenheten styrs av en styrgrupp som beslutar om förvaltningsplan och budget. System är uppdelade på olika förvaltningsgrupper inom ett förvaltningsobjekt.

Informationsklassning: Klassning av informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet.

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det övergripande ansvaret att leda och samordna utvecklingen av kommunens informationssäkerhet.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Ledningssystem: Definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet.

Molntjänster: Tjänster och system som inte drivs lokalt av kommunen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

Nano-learning: Korta återkommande utbildningar som erbjuds för anställda.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.

Personuppgiftsbiträde: Extern fysisk eller juridisk person som skall säkerställa att personuppgifter hanteras säkert och ändamålsenligt för kommunens räkning.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats, tex drift, support och förvaltning av systemet.

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

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.

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.

Säkerhetskopiering: Kopia av den information som finns i en databas eller på en server.