Haninge kommun

Granskning cybersäkerhet
December 2022

Sammanfattning

På uppdrag av Haninge kommuns revisorer har EY genomfört en granskning av kommunens arbete med cybersäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende cybersäkerheten.

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

Granskningen genomfördes från juni till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens cybersäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av cybersäkerhet, "Granskningsprogram Cyber- och Informationssäkerhet" (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter för kommunens cybersäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Haninge kommun ha en genomsnittlig mognadsgrad på 2,60 vilket är jämbördigt med andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Haninge kommun är mognadsgraden klart lägre än vad EY rekommenderar för en kommun likt Haninge. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personuppgiftsstyrning. Kommunens lägsta mognadsgrad är inom området strategi och rutiner.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Haninge kommun tillser att:

- En samordnare rekryteras med informationssäkerhet som sitt huvudsakliga ansvarsområde för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.
- Direktivet för informationssäkerhet färdigställs och beslutas för att säkerställa att den övergripande målbilden och ansvarsfördelningen med informationssäkerhet formaliseras och träder i kraft.
- Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.

Innehållsförteckning

1 Bakgrund

Haninge kommun, i sina 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 cybersäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att information och system är tillgängliga, riktiga samt har tillräckligt starkt skydd.

I sin årliga risk- och konsekvensanalys har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med cybersäkerhet samt risker kopplat till verksamhetskritiska IT-system. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med cybersäkerhet. Riskerna inom dessa områden är inte enbart relaterade till Haninge kommun utan gäller i stor utsträckning hela den offentliga sektorn.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med cybersäkerhet är ändamålsenligt. Vidare är syftet också att bedöma i vilken omfattning kommunstyrelsen styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande övergripande revisionsfråga:

- Bedriver Haninge kommun ett tillräckligt och ändamålsenligt cybersäkerhetsarbete?

Revisionsfrågan bryts ned och besvaras genom följande underliggande revisionsfrågor:

- Kan styrningen av arbetet med cybersäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
  - Görs riskanalyser avseende cybersäkerhet på ett strukturerat sätt och används dessa för att identifiera åtgärder, baserat på upptäckta risker?
  - Finns det en strukturerad metod för att identifiera och skydda kommunens viktigaste informationstillgångar?
  - Har kommunen tillgång till tillräcklig kompetens? Och finns en tillräcklig egen kompetens?
- Är arbetet med att följa upp att beslut och styrdokument relaterat till cybersäkerhet efterlevs ändamålsenligt?
- Är Haninge kommuns incidenthanteringsprocess ändamålsenlig?
  - Finns en förmåga att öva och utbilda utifrån ett krishanteringsperspektiv?

1.2 Avgränsning

Granskningen är avgränsad till att ge en övergripande bild av området och kan även användas till att utgöra en lägesbild och kunskapsunderlag i det fortsatta cybersäkerhetsarbetet.

1.3 Metod och genomförande

Granskningen har byggt på EY:s ramverk för granskning av cyber- 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 cyber- och informationssäkerhet. Information kring områdena har insamlats både genom granskning av relevanta dokument, samt genom att EY:s specialister genomför granskningsmöten med relevanta befattningshavare i kommunen. En bedömning av mognadsgraden har skett på respektive område och angetts på en femgradig skala. Då liknande granskningar genomförs i flera kommuner har såväl en kvantitativ som en kvalitativ jämförelse med andra kommuner genomförts.

Inledningsvis har relevant dokumentation kring kommunens rutiner och processer granskats av EY. Därefter har granskningsmöten med kommunens representanter hållits för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av cyber- och informationssäkerhet i kommuner. Sedan har den samlade bilden av dokumentation samt information inhämtad via granskningsmöten analyserats och bedömts och ett utkast presenterats för kommunens representanter. De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta. Slutligen färdigställdes rapporten och den presenterades för kommunens revisorer vid fastställt revisionssammanträde.

Under granskningen har följande roller intervjuats:

- IT-chef
- Dataskyddsombud
- Säkerhetschef

Fullständig källförteckning av granskad dokumentation framgår av bilaga 1.

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

<u>Styrning</u>

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

<u>Personal och behörigheter</u>

- Personal
- Behörighetshantering

Drift

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar

- Förändringshantering

Personuppgifter

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

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 Haninge kommuns mognadsgrad inom informationssäkerhetsområden

1	Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc
2	Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning
3	Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen
4	Förutom väldokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning
5	Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. 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.

Tidsplanen för arbetet såg ut enligt följande:

Tabell 2: Tidsplan för IT- och informationssäkerhetsgranskningen

Förberedelser och planering	Juni 2022
Insamling och analys av dokumentation	Augusti 2022
Granskningsmöte	September 2022
Rapportskrivning samt intern kvalitetssäkring	September 2022
Faktagranskning av kommunen	September 2022
Justering samt färdigställande av rapport	Oktober 2022
Avrapportering och slutpresentation	December 2022

1.4 Revisionskriterier

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

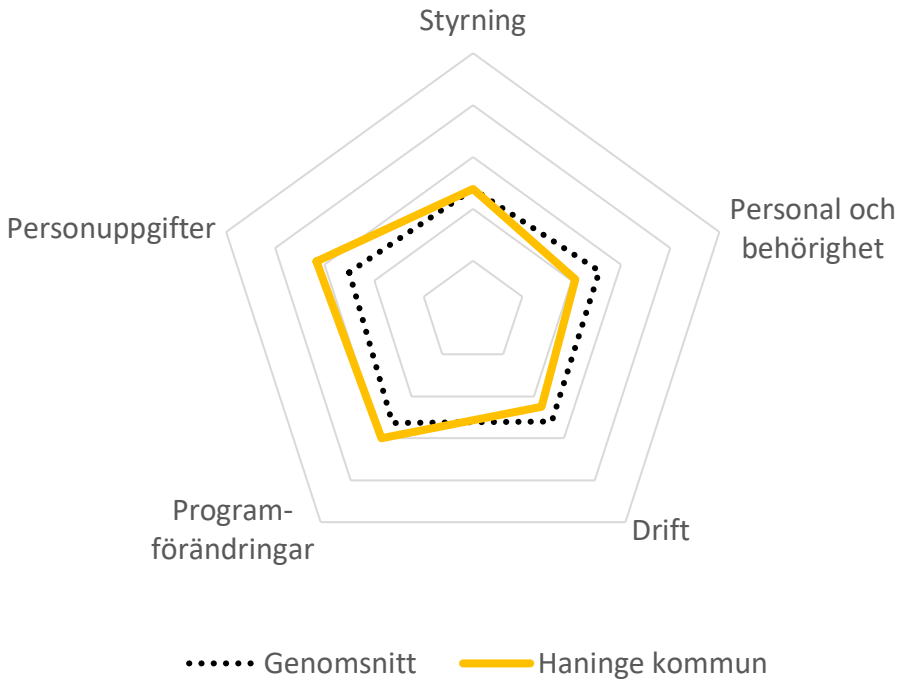
2 Analys

Baserat på den analys och granskning som genomförts bedöms Haninge kommun ha en genomsnittlig mognadsgrad på 2,60 vilket är jämbördigt med andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Haninge kommun är mognadsgraden klart lägre än vad EY rekommenderar för en kommun likt Haninge. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personuppgiftsstyrning. Kommunens lägsta mognadsgrad är inom området strategi och rutiner.

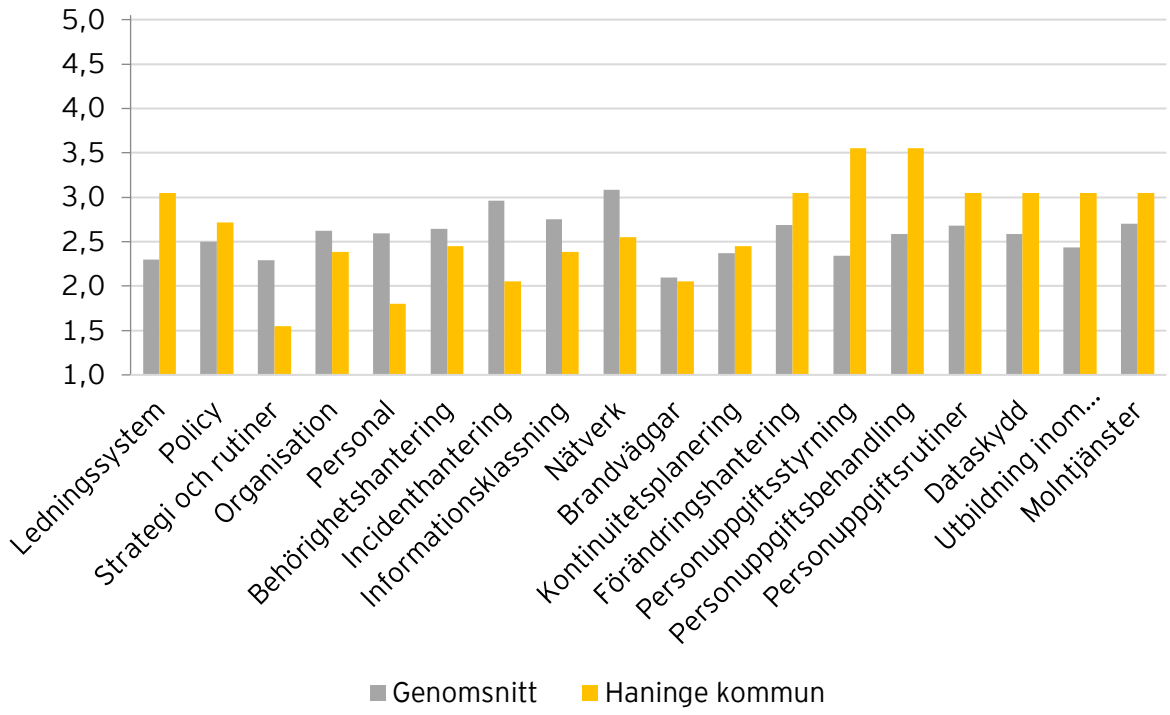
Kommunens främsta förbättringsbehov gäller styrning av informationssäkerhetsarbetet då det vid granskningstillfället saknas formaliserade processer och riktlinjer för flera områden, bland annat utbildningsplan, roll- och ansvarsfördelning och incidenthantering. Därtill har det identifierats ett behov av en utpekad samordnare för informationssäkerheten. Behov för förbättring har även identifierats gällande kommunikation av policy och riktlinjer avseende cybersäkerhet till anställda, samt uppföljning och rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper.

Haninge kommun arbetar aktivt för att utveckla arbetet med cybersäkerhet. Bland annat bedrivs ett arbete för att anställa en informationssäkerhetssamordnare som ska ha övergripande ansvar över informationssäkerheten. Arbete bedrivs även för att ta fram och besluta kring ett informationssäkerhetsdirektiv som ska formalisera styrningen med informationssäkerhet. Därtill ska tillhörande riktlinjer tas fram på tjänstemannanivå som ska beskriva tillvägagångssätt för hur informationssäkerhetsdirektivet ska uppfyllas.

Figur 1 nedan redovisar kommunens mognadsgrad för de 5 huvudområden som granskats samt en jämförelse med andra kommuner av motsvarande storlek och karaktär. Figur 2 visar detsamma fast nedbrutet på 18 underområden. Genomsnittet för andra kommuner av motsvarande storlek och karaktär är framtaget genom att bedöma mognadsgrad för samma områden och enligt samma metod som för Haninge kommun.



Figur 1: Överblick över kommunens mognadsgrad för de 5 huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



Figur 2: Överblick över kommunens mognadsgrad för de 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.

2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se tabell 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet styrning

Område	Nuläge	Iakttagelser	Mognad
Lednings-system	Ett ledningssystem för informationssäkerhet är implementerat i kommunen. Enligt styrdokument för säkerhet och riskhantering inom kommunen (fastställd av kommunfullmäktige oktober 2020) ska informationssäkerhetsarbetet ske utefter svensk etablerad standard. Detta innefattar att tillämpa Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd samt följa tillämpliga delar av den svenska och internationella standardserien ISO/IEC 27000.		3,00
Policy	Kommunfullmäktige har fastställt ett säkerhetsprogram, "Program för säkerhet och riskhantering 2019-2022" som innefattar informationssäkerhet. Programmets övergripande mål är bland annat att leva upp till krav från användare av kommunens tjänster, förhålla sig till lagar och säkerställa godkända interna rutiner. Det beskrivs i säkerhetsprogrammet att kommunstyrelsen följer upp och vid behov reviderar programmet årligen. Vid granskningstillfället bedrivs ett arbete för att etablera ett informationssäkerhetsdirektiv med övergripande mål och riktlinjer för informationssäkerhetsarbetet som ska beslutas på politisk nivå. Direktivet ska konkretisera säkerhetsprogrammet som det övergripande dokumentet för styrning och mål med kommunens informationssäkerhetsarbete. Kommunstyrelsen beslutade 2022-05-09 om en ny digitaliseringspolicy (tidigare IT-policy) som är upprättad av kommunens säkerhetschef. Digitaliseringspolicyn bygger på kommunens alla digitala tjänster och infrastruktur. Vid tid för granskning har ett förslag lämnats på uppdatering av digitaliseringspolicyn som ligger för beslut hos kommunstyrelsen. Det finns ingen definierad frekvens för hur ofta digitaliseringspolicyn ska uppdateras. Det finns en policy för styrdokument som beslutades av kommunfullmäktige 2021-06-14. Policyn beskriver strukturen för styrdokument och syftar till att säkerställa att styrdokument förblir aktuella samt att kommunen inte har fler styrdokument än vad som krävs för att styra verksamheten. Policyn för styrdokument beskriver hur länge ett dokument är giltigt ifall det inte framgår av lagstiftning. Styrdokumenten i kommunen delas in i nivåer, kategorier, beslutnivå och tidsperiod. För övergripande styrdokument är det en långsiktig tidsperiod på minst	Det saknas en definierad frekvens för uppdatering och/eller revision av digitaliseringspolicy för att säkerställa att den förblir riktig och aktuell över tid.	2,67

	10 år, strategiska styrdokument har medellång sikt på 4–10 år och taktisk har en kort sikt på 1–4 år. Dock finns det ingen formaliserad process för att säkerställa att styrdokument uppdateras/revideras enligt tidsintervallet som beskrivs i policyn för styrdokument.	Det saknas formaliserade rutiner för att säkerställa att styrdokument revideras enligt kraven i policyn.	
Strategi och rutiner	Ett utkast för riktlinjer avseende informationssäkerhet har upprättats inom kommunen. Riktlinjerna ska ses som ett minimumkrav för hantering av information och de riktar sig till samtliga medarbetare och förtroendevalda inom kommunen. Enligt intervjuad nyckelperson är utkastet till informationssäkerhets-riktlinjer alltför detaljerat för att beslutas på politisk nivå. Därmed bedrivs ett arbete för att etablera ett informationssäkerhetsdirektiv med övergripande mål och riktlinjer för informationssäkerhetsarbetet som ska beslutat på politisk nivå. För att komplettera informationssäkerhetsdirektivet ska specifika riktlinjer och instruktioner (som beskriver hur arbetet ska bedrivas för att leva upp till krav- och målbild) tas fram och beslutas på tjänstemannanivå. Enligt intervjuad nyckelperson kommer direktivet och kompletterande styrdokument bygga på utkastet till riktlinjer för informationssäkerhet. Enligt intervjuad nyckelperson ska det framöver finnas ett informationssäkerhetsråd för att säkerställa att informationssäkerhetsarbetet sker effektivt. Genom informationssäkerhetsrådet ska kommunen bygga fram en systematik kring informationssäkerhetsarbetet som inte finns på plats vid granskningstillfället. Det finns en förvaltningsstyrningsmodell inom kommunen som stödjer det kommungemensamma arbetet med förvaltning och utveckling av IT-stöd. Förvaltningsstyrningsmodellen bygger på modellen pm3. Förvaltningsstyrningsmodellen syftar till att bidra till bland annat IT-stöd, kontroll över kostnader och tydliggöra förvaltningsorganisationens ansvar. Kommunens förvaltningsstyrningsmodell sågs över under 2021 och vid granskningstillfället finns ett förslag för att förbättra och mer tydligt förankra förvaltningsstyrningsmodellen i kommunens verksamheter. Förslaget ska bidra till ett mer systematiserat arbete med tydligare mandat och bättre möjligheter att följa upp arbetet. Det finns dokumenterade riktlinjer för hantering av IT-relaterade produkter och tjänster inom kommunen. Riktlinjerna innefattar bland annat IT-säkerhet, styrning av IT samt målsättning med IT-arbetet. De nuvarande riktlinjerna avseende IT fastställdes under 2022 och enligt intervjuad nyckelperson uppdateras de varje år.	Det saknas riktlinjer för informationssäkerhet som på tjänstemannanivå beskriver hur arbetet inom kommunen ska bedrivas för att leva upp till ändamålsenlig informationssäkerhet. Det saknas en systematik kring kommunens styrning av informationssäkerhet.	1,50

	Enligt utkast till riktlinjer för informationssäkerhet ska policy och riktlinjer kontinuerligt förankras hos medarbetare. Metoder och ansvar för kommunikation av policy och riktlinjer är däremot inte dokumenterade. Enligt intervjuad nyckelperson finns policy och riktlinjer tillgängliga för samtliga medarbetare på kommunens intranät och det är individens ansvar att gå på in på intranätet och läsa styrdokumenten. Enligt intervjuad nyckelperson bedrivs även ett arbete för att utveckla introduktionsutbildningen för nyanställda för att säkerställa att nyanställda arbetar med säkerhetsaspekter utefter kommunens policy och riktlinjer. Vid granskningstillfället nås dock inte medarbetare aktivt av styrdokumenten och det finns inga formella krav på att anställda ska ta del av och vara införstådda med policy och riktlinjer avseende informationssäkerhet.	Det saknas ett systematiskt arbetssätt för att säkerställa att medarbetare har kännedom om kommunens styrdokument avseende IT- och informationssäkerhet.	
Organisation	Kommunens säkerhetsarbete är decentraliserat, det vill säga att kommunstyrelsen leder, samordnar och utvecklar ett område medan nämnder och förvaltningar ansvarar för att säkerhetsarbetet bedrivs ändamålsenligt. Enligt intervjuad nyckelperson finns det en problematik i den decentraliserade modellen då det kan ta lång tid från att säkerhetsenheten har identifierat ett problem till dess att det blir implementerat i nämnder/verksamheter. Vidare förekommer det ingen systematisk rapportering till kommunstyrelse avseende hur cybersäkerhetsarbetet fortlöper. Kommunens säkerhetsprogram beskriver att kommunfullmäktige fastställer den övergripande målsättningen för säkerhetsarbetet medan kommunstyrelsen har det övergripande ansvaret för att säkerhetsarbetet leds, utvecklas och bedrivs effektivt. Därtill är det kommunstyrelseförvaltningens roll att verkställa kommunstyrelsens uppdrag. Utförlig roll- och ansvarsfördelning för Haninge kommuns informationssäkerhetsarbete stipuleras i kommunens utkast till riktlinjer för informationssäkerhet. I utkastet framgår det att kommunstyrelsen sätter upp mål och ramar för informationssäkerhetsarbetet samt ansvarar för att det uppnås. Enskilda nämnder ansvarar för att informationssäkerhetsarbetet sker på ett korrekt sätt enligt kommunstyrelsens anvisningar. Verksamhetsansvarig är den ansvariga för säkerheten inom respektive verksamhetsområde. Det genomförs ingen central formaliserad uppföljning av hur väl nämnder och verksamheter efterlever policy och riktlinjer avseende cybersäkerhet. Enligt intervjuade nyckelpersoner ska roll- och ansvarsfördelningen som beskrivs i förslaget av riktlinjer för informationssäkerhet finnas beskrivet i	Kommunens organisationsstruktur leder till fördröjningar mellan identifierat problem och implementation av lösning. Det saknas en process för kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Det saknas en formaliserad process för uppföljning och kontroll av hur väl anställda inom kommunen efterlever policy och riktlinjer avseende cybersäkerhet. Roll- och ansvarsfördelningen kring informationssäkerhet	2,33

	nya direktivet för informationssäkerhet. Vid granskningstillfället är dock roll- och ansvarsfördelning för samtliga roller inom kommunens arbete med informationssäkerhet inte beskrivet i styrande dokument. Ansvarsområden för kommunens IT-enhet finns dokumenterade i en Samverkanshandbok. Det beskrivs i handboken att IT-enheten ansvarar bland annat för kravställning och uppföljning av externa driftleverantörer. Dessutom ansvarar IT-rådet för planering, genomförande, förankring och lansering av styrdokument inom IT-området, samt säkerställande av att riktlinjer avseende IT efterlevs. Kommunens ansvar och roller för hantering av personuppgifter finns dokumenterat i kommunens riktlinjer för GDPR. I riktlinjerna framgår det vilket ansvar som dataskyddsombud, kommunstyrelsen, nämnder, dataskyddskoordinator, medarbetare och chefer besitter. Det beskrivs bland annat att ett dataskyddsombud ska utses av kommunens samtliga nämnder, kommunstyrelse och bolag. Dataskyddsombudet har som uppgift att ge råd vid frågor kring personuppgiftbehandling och samråda vid personuppgiftincidenter och konsekvensbedömningar. Vidare övervakar dataskyddsombudet personuppgiftsansvarigas arbete i behandling av personuppgifter och är kontaktperson gentemot integritetsmyndigheten och medborgarna. Dataskyddsombudet har direkt kontakt med kommunens dataskyddskoordinatorer som har ansvar för sin respektive nämnd. Budgeten avsedd för informationssäkerhet är inte fixerad gentemot verksamhetens och IT:s budget, utan följer de informationssäkerhetsbehov som finns och uppstår. Budgeten följs upp enligt kommunens budgeteringsprocess som finns beskriven i "Leveransmodell årshjul mötesforum leverantörsstyrning". Enligt IT-riktlinjer ska det ställas krav på externa leverantörer för att säkerställa att verksamheternas behov är i centrum. Kommunen har en kravspecifikation vid upphandling tekniska kravställningar på leverantörer som ska beaktas vid upphandling. Kravspecifikationen inkluderar krav på bland annat IT-säkerhet, behörighet och autentisering. Vid upphandling uppmanas beställaren i kommunens verksamhet att diskutera kraven med IT-enheten för att säkerställa att kraven uppfyller kommunens standardiserad IT-infrastruktur. Enligt intervjuad nyckelperson finns det ingen formaliserad process för att säkerställa att IT-enheten informeras inför upphandling av verksamhetssystem. Därmed har det	innefattar inte samtliga roller inom kommunens informationssäkerhetsarbete. Det saknas en formaliserad process som säkerställer att verksamheter inte kan upphandla system utan IT-enhetens kännedom.	

	hänt att verksamhetssystem upphandlas utan IT-enhetens kännedom. Processen för upphandling av informationssystem och hantering av leverantörsavtal är decentraliserad enligt intervjuad nyckelperson, där ansvaret ligger på systemägaren. Enligt intervjuad nyckelperson har kommunen leverantörsforum där kommunens IT-enhet träffar leverantörer veckovis på operativ nivå och 1–2 gånger per år på strategisk nivå. För SLA, incidenter och beställningar sker uppföljning månadsvis.		

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 4).

Tabell 4: Nuläge och iakttagelser inom huvudområdet personal och behörigheter

Område	Nuläge	Iakttagelser	Mognad
Personal	Enligt intervjuad nyckelperson finns ett behov av ytterligare resurser och mognad inom kommunens informationssäkerhetsfunktion. Kommunens informationssäkerhetsarbete ligger under säkerhetsenhetens ansvar och kommunens säkerhetssamordnare är utpekad samordnare för informationssäkerhet, men säkerhetssamordnaren har även andra arbetsuppgifter utöver informationssäkerhet. Enligt intervjuad nyckelperson finns ett behov av en utpekad informationssäkerhets-samordnare som enbart har informationssäkerhet som sitt ansvarsområde. Vid granskningstillfället bedrivs ett arbete för att anställa en informationssäkerhets-samordnare. 2021-04-08 tog kommundirektören beslut om ny rutin gällande bakgrundkontroll som började gälla från 1 maj 2021. Bakgrundskontroll ska genomföras för rekrytering till IT- och informationssäkerhets funktionen då dessa anses vara nyckelfunktioner. Enligt intervjuade nyckelpersoner är säkerhetsenheten i behov av stöd i rekryteringen till anställningar kopplade till cybersäkerhet då kommunen saknar en formaliserad process för rekrytering. Enligt dokumenterade IT-anvisningar uppmanar kommunen medarbetare att genomföra Disa (MSB:s digitala grundutbildning i informationssäkerhet). Den digitala utbildningen är inte obligatorisk för kommunens anställda. Enligt intervjuad nyckelperson är ambitionen inom kommunen att samtliga anställda	Det saknas en informationssäkerhets-samordnare som har informationssäkerhet som sitt huvudsakliga ansvarsområde.	1,75

	inom IT- och informationssäkerhetsfunktionen ska genomföra grundutbildningen och att deltagande ska följas upp. Utbildning inom informationssäkerhet ska även bli en del av introduktionsprogrammet för nyanställda. Vid rekrytering av informationssäkerhets-samordnare ska det ligga under dennes ansvar att följa upp och säkerställa att samtliga medarbetare som hanterar kommunens information är tillräckligt utbildade. Vid granskningstillfället finns dock inte en dokumenterad plan för kontinuerliga och obligatoriska utbildningstillfällen kopplat till cybersäkerhet. Enligt intervjuade nyckelpersoner har samtliga kommunens IT-system en utsedd systemägare. I förvaltningsobjektsarkitekturmodellen finns en lista över kommunens samtliga system, där systemägare för respektive system finns beskrivet.	Det saknas en dokumenterad utbildningsplan för cybersäkerhet.	
Behörighets-hantering	Kommunen har en definierad process för behörighetshantering som beskrivs i dokumenterade instruktioner för hur användarkonton ska administreras. Instruktionen beskriver hur olika typer av användarkonton skapas och administreras inom kommunen, bland annat anställd, vikarie, konsult och vårdnadshavare. Enligt instruktionen är det den anställdas chef som begär att skapa ett användarkonto och väljer vilka behörigheter och system som ska tilldelas den anställda. Enligt intervjuad nyckelperson måste personen vara registrerad i kommunens lönesystem för att få tillgång till ett användarkonto. Detta säkerställer att endast anställda kan få tillgång till kommunens system. Avslut av behörighet sker automatiskt vid avslut av tjänst då samtliga behörigheter är kopplade till kommunens HR-system. Efter den anställdas sista arbetsdag avslutas användarkontot automatiskt och därmed försvinner samtliga behörigheter kopplade till användaren. Användarbehörigheter på infrastrukturell nivå tilldelas av leverantör till respektive system. Endast ServiceDesk kan ha kontinuerlig admin-rättighet. Lokala tekniker inom specifik nämnd/verksamhet kan tilldelas temporär admin-rättighet för en viss uppgift. Ingen anställd inom kommunens kan tilldela höga behörigheter eftersom kommunen inte äger någon infrastruktur, varvid infrastrukturen hanteras av extern driftleverantör. Enligt intervjuad nyckelperson genomförs uppföljningar på vilka som har höga behörigheter och säkerhetsenheten får rapporter på vilka som läggs till eller tas bort på infrastrukturell nivå. Processen för periodisk genomgång av behörigheter är inte central då respektive systemägare bestämmer		2,40

	själv hur behörigheter ska styras. Enligt intervjuad nyckelperson ska olämpliga behörigheter upptäckas under klassning av system vilket ska ske minst vartannat år. Det genomförs däremot ingen specifik periodisk genomgång av samtliga behörigheter som hanterar kommunens informationstillgångar. Vid tid för granskning finns det ingen dokumenterad process för att säkerställa en lämplig segregering av roller och behörigheter inom både organisationen och informationssystemen. Enligt intervjuade nyckelpersoner ligger det på respektive systemägare att säkerställa att roller inom systemet är lämpligt segregerade, men varken process eller ansvar är formaliserat och dokumenterat. Lösenordskraven för kommunens system beskrivs i IT-riktlinjerna. Enligt intervjuad nyckelperson är det inte tekniskt möjligt att ha ett lösenord som inte lever upp till lösenordskraven. För majoriteten av kommunens system sker inloggning genom single-sign-on (SSO) via Active Directory, vilket innebär att användare inte har ett separat lösenord för dessa system. Enligt intervjuade nyckelpersoner gäller SSO för samtliga verksamhetskritiska system. Det förekommer dock system inom kommunen med separat inloggning. För dessa system sker det ingen kontroll för att säkerställa att användares lösenord överensstämmer med kommunens lösenordskrav.	Det saknas kravställning mot systemägare att periodisk genomgång av behörigheter ska genomföras för samtliga användare som hanterar kommunens informationstillgångar. Det saknas en formaliserad process för att säkerställa lämplig segregering av roller inom organisationen och kommunens system. Det saknas en process för att säkerställa att samtliga kommunens system lever upp till lösenordskraven.	

2.3 Drift

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

Tabell 5: Nuläge och iakttagelser inom huvudområdet drift

Område	Nuläge	Iakttagelser	Mognad
Incident-hantering	Enligt utkast till riktlinjer för informationssäkerhet ska säkerhetsincidenter som misstänks kunna påverka informationssäkerheten rapporteras i kommunen incidenthanteringsverktyg KIA där det automatiskt går till närmsta chef utan dröjsmål. Enligt intervjuad nyckelperson har samtliga anställda möjlighet att rapportera en säkerhetsincident. Dokumentation som beskriver kommunens hantering av informationssäkerhetsincidenter ska enligt intervjuad nyckelperson framgå i det nya direktivet för informationssäkerhet. Vid tid för granskning finns det dock ingen beslutad dokumentation som beskriver hantering av informationssäkerhetsincidenter. För IT-säkerhetsincidenter finns det instruktioner dokumenterade i IT-anvisningar och -riktlinjer att vid	Det saknas dokumentation som beskriver hantering av informationssäkerhets-incidenter.	2,00

	misstanke eller upptäckt av en säkerhetsincident ska det rapporteras till närmsta chef samt IT-enheten omedelbart. Hantering av IT-säkerhetsincidenter beskrivs även i kommunens Incident management process där en incident definieras som ett oplanerat avbrott och reducering i kvaliteten i en IT-tjänst eller fel på konfigurationsenhet i en IT-tjänst. Incident Management-processen är baserad på fyra (4) delområden: identifiering, analys, åtgärd samt framtida lösningar. Processen används för att standardisera rutiner för en snabb åtgärd, analys, dokumentation och rapportering. Incidenter följs upp veckovis inom respektive operativt forum och nyckeltal följs upp i strategiskt och taktiskt forum. Det finns även en Major incident management process som beskriver hantering av kritiska incidenter samt definierar roller och ansvar kopplade till kritiska incidenter. Efter att en major incident är löst ska en incidentrapport skrivas av Major Incident Manager enligt en framtagen mall. Major incidenter följs också upp veckovis i operativt forum. Det finns en Problem management process som kompletterar kommunens riktlinjer kring IT-incidenthantering. Problem management-processen används för att finna en permanent lösning på problem som uppstår och finna den underliggand grundorsaken till de incidenter som uppstår. Enligt intervjuad nyckelperson sker det inte någon direkt kommunikation till anställda om hur de ska agera vid upptäckt av IT-incident utan det är individens ansvar att ta del av riktlinjer och information som finns tillgängligt för samtliga anställda på kommunens intranät.	Det saknas direkt kommunikation av riktlinjer avseende IT-incidenter för att säkerställa att anställda är medvetna om hur de ska gå tillväga vid upptäckt av IT-incident.	
Informations-klassning	Det finns en instruktion för klassning av kommunens informationstillgångar som följer en klassificeringsmodell som bygger på riktighet, tillgänglighet, spårbarhet och konfidentialitet (sekretess) av information. Klassningsnivåerna går från 1 till 3 och definieras utefter den uppskattade skadan. De tre nivåerna är uppskattad måttlig skada, betydande skada eller allvarlig skada. Enligt dokumenterad utkast till riktlinjer för informationssäkerhet ska samtliga av kommunens IT-system och tjänster som hanterar information klassificeras. Det framgår även ur IT-anvisningar och -riktlinjer att samtliga verksamhetssystem ska informationsklassas vid upphandling. Enligt intervjuad nyckelperson genomförs klassning i verktyget KLASSA, men det saknas konkret och dokumenterad styrning av informationsklassning då det är upp till respektive systemägare att säkerställa att		2,33

	informationsklassning utförs. Styrning av informationsklassning ska formaliseras i det nya direktivet för informationssäkerhet då det ska framgå att samtliga system ska klassas minst vartannat år. Det beskrivs i kommunens utkast till riktlinjer för informationssäkerhet att varje verksamhet ska genomföra riskanalys för sina respektive processer och IT-system. Det framgår att riskanalys ska som minimum genomföras vid etablering av IT-system samt vid förändringar i organisation, process, infrastruktur eller programvaror. Riktlinje avseende riskanalys är vid granskningstillfället inte dokumenterat i beslutad dokumentation och det finns ingen processbeskrivning av hur en riskanalys ska genomföras.	Det saknas en dokumenterad riktlinje som beskriver när en riskanalys ska genomföras. Det saknas en processbeskrivning av hur en riskanalys ska genomföras.	
Nätverk	I Haninge Kommun är det externa leverantörer som driftar nätverken men Haninge kommuns IT-enhet har som ansvar att koordinera mellan de olika leverantörerna. Enligt intervjuad nyckelperson träffas kommunens förvaltningsledare för nätverk med leverantörerna kontinuerligt. Kravställningen på enskilda leveranser definieras vid upphandling. Inom kommunen finns det inget beslutat dokument som beskriver styrning av kommunens nätverksmiljö. Både intrusion detection system och intrusion prevension system är implementerat för att analysera kommunens nätverksaktivitet.	Det saknas dokumenterad styrning/kravställning på kommunens nätverksmiljö.	2,50
Brandväggar	Kommunens brandväggar styrs av leverantör men det finns ingen dokumentation för styrning av brandväggar inom kommunen då styrningen utgår ifrån leverantörens kompetens och certifieringar inom brandväggar. Enligt intervjuad nyckelperson rensas överflödiga brandväggsregler kontinuerligt. Kommunens brandväggskonfigurationer granskas dock inte på regelbunden basis.	Det saknas dokumenterad styrning/kravställning på kommunens brandväggar. Det saknas en process som regelbundet säkerställer att brandväggarnas konfigurationer förblir lämpliga över tid.	2,00
Kontinuitetsplanering	Kommunen har en dokumenterad plan för extraordinära händelser för IT-enhetens centrala leveranser. Syftet med planen är främst information om IT-enhetens centrala leveranser och hur deras leverantörer ska hantera ett avbrott, störning eller en cyberattack. Syftet med planen är att säkerställa att kommunen har en god krishanteringsförmåga. Kommunen har även definierat vad som beteckar en katastrof eller kris i kommunens program för säkerhet och riskhantering. Enligt intervjuad nyckelperson har kommunen driftdokumentation för verksamhetskritiska system. Vid granskningstillfället sker inte någon central uppföljning för att säkerställa att driftdokumentation	Det saknas en process som säkerställer att	2,40

	finns på plats för samtliga verksamhetskritiska system. IT-enheten har möjlighet att kontrollera att driftdokumentationen finns på plats men det är inget som sker systematiskt då ansvaret ligger på respektive verksamhet. I kommunens kontinuitetsplan för IT-enhetens centrala leveranser är det beskrivet att alla förvaltningar ska ta fram en egen kontinuitetsplan för sin respektive verksamhet. Kommunens IT-enhet varit till stöd för förvaltningarna med att ta fram individuella kontinuitetsplaner. Enligt intervjuad nyckelperson har en individuell kontinuitetsplan tagits fram för de flesta verksamheter men det är inte färdigställt för samtliga. Ansvaret att upprätta kontinuitetsplan ligger på respektive förvaltning/verksamhet. Kommunens IT-enhet kan ha koll på vilka verksamheter som har upprättat kontinuitetsplan men det genomförs ingen uppföljning för att säkerställa att kontinuitetsplan har upprättats. Enligt intervjuad nyckelperson är det förvaltningsledarens ansvar att kommunicera kontinuitetsplan till anställda inom förvaltningen. Det sker ingen central uppföljning för att säkerställa att anställda har kännedom om kontinuitetsplanen för sin verksamhet. Kommunen tillhandahåller en modell för risk- och sårbarhetsanalys för åtgärder för extraordinära händelser. Modellen är indelad i sex olika scenarion där varje scenario är uppdelat i tre olika steg. Ytterligare ska de processer och system som är kritisk för verksamheten identifieras utifrån tio olika delar. Slutligen ska en krisplan identifieras.	driftdokumentation finns på plats för samtliga verksamhetskritiska system. Det saknas ett formaliserat arbete för att säkerställa att ändamålsenlig kontinuitetsplan upprättas för kommunens samtliga förvaltningar/verksamheter. Det saknas en dokumenterad process för att säkerställa att anställda har kännedom om kontinuitetsplanen för sin verksamhet.	

2.4 Programförändringar

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

Tabell 6: Nuläge och iakttagelser inom huvudområdet programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Kommunen har dokumentation som beskriver processen för förändringshantering både på intranätet och i en Change management process. Det finns även ett separat dokument vid namn "Förändringshanting för leverantörer" som beskriver hur förändringar från leverantörer ska hanteras och genomföras. Därtill finns en Leveransmodell för Change management-process vilken är en standardiserad metod som beskriver hur kommunen effektivt ska hantera förändringar i IT-infrastrukturen.		3,00

	Enligt intervjuad nyckelperson genomförs inga stora förändringar inom kommunen då det främst är färdigutvecklade system som köps in, där krav avseende gränssnitt ställs på leverantören vid upphandling. Inom kommunen genomförs dock viss programförändring/-utveckling. Förändringar i kommunens samtliga IT-system följer förändringsprocessen ITIL V3. Programförändringar beslutas genom veckovisa Change Advisory Board (CAB) där ärenden anmäls minst två (2) dagar innan. Det finns även en Emergency Change Advisory Board för beslut som anses vara tillräckligt allvarliga för att vänta tills ett ordninare CAB-möte. Enligt intervjuad nyckelperson finns det ingen dokumenterad styrning av patchningar. Det finns inte heller någon lista på genomförda respektive avböjda patchningar, men en lista kan genereras från leverantör vid efterfrågan. Enligt intervjuade nyckelpersoner finns det ingen separation mellan utvecklings-, test- och produktionsmiljö utan flera verksamhetssystem testas direkt i produktionsmiljö. För centrala IT-system finns test-miljö där förändringar testas innan de implementeras i produktionsmiljö.	Det saknas dokumenterad styrning av patchningar. Det saknas separation och styrning av utvecklings-, test- och produktionsmiljö för verksamhetssystem.	

2.5 Personuppgifter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personuppgifter* samt de iakttagelser som noterats under granskningens utförande (se tabell 7).

Tabell 7: Nuläge och iakttagelser inom huvudområdet personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts-styrning	Kommunen har dokumenterade riktlinjer avseende hantering av personuppgifter som beskriver att personuppgifter inom kommunen ska hanteras enligt gällande regler i dataskyddsförordningen. Riktlinjerna innefattar samtliga områden inom kommunens personuppgiftsarbete, dvs. rollbeskrivning, personuppgiftsbehandling, säkerhet, konsekvensbedömning, personuppgiftsbiträden, personuppgiftsincident samt registrerades rättigheter. Riktlinjerna ska tillämpas av samtliga verksamheter i kommunen. Enligt intervjuade nyckelpersoner sker det ingen systematisk uppdatering av riktlinjen för GDPR, utan riktlinjen uppdateras när ett behov upptäcks. I kommunens program för säkerhet och riskhantering 2019-2022 framgår det hur kommunen ska arbeta med personuppgiftsäkerhet. I de fall kommunen har bristande informations- och personuppgiftsäkerhet kan	Det saknas en process för att systematisk säkerställa att riktlinjer för GDPR förblir riktiga och aktuella över tid.	3,50

	det medfölja störningar i samhällsviktiga verksamheter och att viktig information går förlorad eller stjäls. I programmet framgår det att personuppgifter och den personliga integriteten ska skyddas genom högt dataskydd och behandling av personuppgifter ska ske ändamålsenligt och lagligt. Vidare yttras det i programmet att anställda, leverantörer och utomstående användare ska ha kunskap inom informationssäkerhetsregler och personuppgiftshantering enligt GDPR. Enligt intervjuad nyckelperson har specifika verksamheter egna lokala riktlinjer som är anpassade efter verksamheten i de fall då centrala riktlinjer inte är optimala eller applicerbara. Det ingår i den årliga egenkontrollen att rapportera till DSO hur väl specifika rutiner som finns för hanteringen av personuppgifter efterlevs och om de behöver förbättras. Varje år ska alla kommunens nämnder genomföra egenkontroll på dataskyddsarbetet inom nämnden och rapportera resultatet av kontrollen till DSO. Egenkontrollen inkluderar bland annat att kontrollera att nuvarande rutiner är tillräckliga, att medarbetare har blivit utbildade samt att konsekvensbedömning har genomförts för relevanta personuppgiftsbehandlingar. Egenkontrollen kan inkludera stickprovskontroll för att säkerställa efterlevnad av GDPR. Rutinen för egenkontroll och återrapportering av GDPR-arbetet inom varje nämnd är dokumenterad och beslutad av kommundirektören. Dataskyddsombudet skriver årligen en rapport till kommunstyrelsen om kommunens GDPR-arbete med syfte att beskriva hur kommunen efterlever GDPR. GDPR-rapporten för 2021 beskriver kommunens organisation avseende GDPR samt personuppgiftincidenter och åtgärder som genomförts under 2021. Rapporten inkluderar även dataskyddsombudets bedömning och rekommendationer för 2022, vilka inkluderar bland annat att vidare öka kunskapen avseende lagstiftningen och tydlig ansvarsfördelning.		
Personuppgifts-behandling	Riktlinjer för personuppgiftsbehandling beskrivs i kommunens riktlinjer för GDPR. Kommunens personuppgiftsbehandlingar registreras i kommunens system för registerförteckning (Draft-it) som innefattar cirka 400 personuppgiftsbehandlingar. Enligt riktlinjer för GDPR ska varje behandling av personuppgifter registreras i registerförteckningen där dataskyddskoordinatorn på respektive nämnd ansvarar för att granska och säkerställa att personuppgiftsbehandlingen registrerats korrekt. Det genomförs årlig egenkontroll av personuppgiftsbehandlingar i respektive nämnd för att		3,50

	säkerställa att dataskyddsarbetet bedrivs ändamålsenligt. Genomförande av konsekvensbedömning för personuppgiftsbehandling beskrivs i riktlinjer för GDPR. Kommunen följer ett verktyg för att genomföra konsekvensbedömning för personuppgifts-behandlingar. I konsekvensbedömning besvaras flera frågor inom kategorierna grundläggande, ändamål & rättslig grund, typer av personuppgifter, information till de registrerade, registrerades rättigheter, överföringar och mottagare samt säkerhet och incidenthantering. Konsekvensbedömningen klassificeras antingen som låg, medel eller hög där det även framgår hur många risker som är identifierade, pågående och åtgärdade. Konsekvensbedömningen genomförs i samband med att personuppgifts-behandlingen registreras och dataskyddskoordinatorn ser över konsekvensbedömningen för att säkerställa att den fyllts i korrekt.		
Personuppgifts -rutiner	Kommunens hantering av personuppgifter och registrerades rättigheter enligt GDPR finns beskrivet på kommunens intranät samt i riktlinjer för GDPR. På kommunens hemsida finns en blankett för begäran om registerutdrag. Ut begäran av registerutdrag kontrolleras inte personens identitet, men registerutdraget skickas endast till personens folkbokföringsadress. Kommunen har dokumenterade instruktioner för hantering av personuppgiftsincident. Vid misstanke eller upptäckt om att en personuppgiftsincident har inträffat ska den som upptäcker incidenten alltid rapportera det i kommunens incidentrapporterings-system KIA samt rapportera det till sin närmsta chef. Personuppgiftsincidenter loggförs i KIA för att hålla koll på antalet incidenter som uppstår. Kommunens dataskyddsombud får anmälan automatiskt och ska samråda vid personuppgiftsincident. Om personuppgiften eventuellt medför risk för fysiska personers rättigheter och/eller frihet ska det rapporteras till tillsynsmyndigheten inom 72 timmar och personuppgiftsansvarig ska utan dröjsmål informera den berörda personen. Processen för hantering av personuppgiftsincidenter kommuniceras till medarbetare genom personuppgiftsutbildning samt att informationen finns på kommunens intranät som är tillgänglig för samtliga medarbetare. Enligt intervjuad nyckelperson ska arkivering av personuppgifter ske enligt respektive nämnds dokumenthanteringsplan som ställer krav på hur länge information måste sparas. Den ansvarige för respektive system ska säkerställa att personuppgifter i systemet lagras utefter respektive dokumenthanteringsplan. Vidare är det den ansvariga		3,00

	för respektive personuppgiftsbehandling som avgör hur länge personuppgiften behöver sparas och när den måste gallras. Den ansvarige för systemet där personuppgiften lagras är ansvarig för att ta fram rutiner för gallring som beskriver när, hur och av vem som uppgiften ska gallras. När dataskyddskoordinatorn går igenom Draft-it ska det framgå ifall en gallringsrutin är framtagen för respektive personuppgiftsbehandling. Det finns dock ingen formaliserad rutin på plats för att säkerställa att gallringsrutiner har tagits fram för kommunens samtliga personuppgiftsbehandlingar.	Det finns ingen formaliserad rutin på plats som säkerställer att det finns dokumenterade gallringskrav för samtliga personuppgiftsbehandlingar.	
Dataskydd	Kommunens arbete med dataskydd beskrivs i riktlinjen för GDPR. Kravet på dataskydd innebär att personuppgifter inte behandlas i onödan. För att skydda personuppgifter som hanteras inom kommunen ska personuppgiftsansvariga skydda registrerades personuppgifter med tekniska och organisatoriska säkerhetsåtgärder som säkerställer en lämplig säkerhetsnivå. Därtill bör principen om inbyggt dataskydd beatrakts vid upphandling av IT-system samt under hela IT-systemets livscykel. Teknisk hantering av personuppgifter beskrivs i kommunens IT-handbok. Enligt intervjuade nyckelpersoner används IT-handboken som stöd för att bedöma vilka åtgärder som krävs för att förbättra dataskyddsarbetet.		3,00
Utbildning inom dataskydds-förordningen	Enligt intervjuad nyckelperson genomfördes en obligatorisk Nano-utbildning kring GDPR för samtliga anställda när GDPR trädde i kraft. Många nya som börjar arbeta för kommunen genomför en grundutbildning inom GDPR och det finns även information om kommunens arbete kring GDPR på intranätet. För ytterligare utbildning är det verksamhetschefernas ansvar att se till att samtliga anställda inom verksamheten är utbildade kring GDPR och har tillräcklig kunskap för att efterleva riktlinjer kring GDPR. Det genomförs årlig uppföljning av hur välutbildade anställda inom kommunen är inom GDPR genom nämndernas egenkontroll av dataskyddsarbetet. I egenkontrollen beskriver respektive nämnd hur utbildningar har genomförts samt resultat av utbildningarna. Det finns dock ingen kravställning på kommunens nämnder och verksamheter att utbildning inom personuppgiftshantering ska vara obligatoriskt för samtliga anställda som hanterar kommunens information. Under granskningen har det observerats att det förekommer anställda inom kommunen som ej genomgått utbildning i dataskyddsfrågor.	Det finns ingen central kravställning på att samtlig personal som hanterar kommunens information ska ha genomfört utbildning inom personuppgiftshantering.	3,00
Molntjänster	Enligt riktlinje får information ej sparas på externa molnlagringsytor om inte dessa har genomgått riskanalys och blivit godkända av verksamheten samt att skyddsåtgärder såsom kryptering har vidtagits. Enligt intervjuad nyckelperson ska pub-avtal enligt SKR:s avtalsmall upprättas med samtliga leverantörer som hanterar kommunens personuppgifter. Avtalen		3,00

	innefattar krav på att kommunens personuppgifter endast får hanteras och lagras utanför EU/EES vid skriftligt godkännande från kommunen. Det framgår även ur IT-anvisningar att känsliga personuppgifter inte får lagras i molntjänsten Microsoft Teams. Tekniska krav på molntjänstleverantörer ställs via kommunens kravspecifikation för upphandling av nya system. I kravspecifikationen för molntjänster ställs krav på att molntjänst-systemet ska vara tillgängligt som tjänst där bland annat drift, övervakning, support och säkerhetskopiering ingår. Därtill ska leveransen ske inom EU/EES. Om en molntjänstleverantör lyder under utländsk lagstiftning som inte lever upp till GDPR krävs ytterligare utvärdering från leverantören för att säkerställa att lämpliga skyddsåtgärder vidtas samt att GDPR efterlevs.		

3 Övergripande rekommendationer

Granskningen har identifierat iakttagelser inom flera delar av ramverket. EY har valt att presentera de mest relevanta rekommendationerna för Haninge kommun och förslag på åtgärder för de främsta riskerna inom IT- och informationssäkerhetsarbetet.

Främst rekommenderar EY att kommunstyrelsen i Haninge kommun tillser att:

- En samordnare rekryteras med informationssäkerhet som sitt huvudsakliga ansvarsområde för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.
- Direktivet för informationssäkerhet färdigställs och beslutas för att säkerställa att den övergripande målbilden och ansvarsfördelningen med informationssäkerhet formaliseras och träder i kraft.
- Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.
- En riktlinje för hantering av informationssäkerhetsincidenter upprättas och beslutas för att formalisera arbetsmetoder och säkerställa att anställda inom kommunen följer en enhetlig process som är ändamålsenlig.
- En ändamålsenlig kontinuitetsplan finns på plats för samtliga kommunens verksamheter. Kommunstyrelsen bör även tillse att en process upprättas som regelbundet säkerställer att kontinuitetsplanerna förblir riktiga och aktuella över tid.

Därefter rekommenderar EY även att kommunstyrelsen i Haninge kommun tillser att:

- En utbildningsplan för cybersäkerhet upprättas och beslutas. Utbildningsplanen bör innehålla obligatoriska och regelbundna utbildningar för samtliga anställda som hanterar kommunens information och deltagande bör följas upp för att säkerställa att samtliga berörda anställda har genomfört utbildningarna.
- En formaliserad internkontrollplan upprättas, beslutas och implementeras för att granska och säkerställa att policy och riktlinjer avseende cybersäkerhet efterlevs i praktiken. Interkontrollplanen bör även inkludera uppföljning av GDPR från centralt håll som inte förlitar sig på att kommunens nämnder granskar sitt eget personuppgiftsarbete.
- Formaliserade rapporteringskrav kring cybersäkerhet upprättas, beslutas och implementeras för att säkerställa kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Den kontinuerliga rapporteringen tillåter kommunstyrelsen att identifiera gap och kontrollera efterlevnad av policy och riktlinjer avseende cybersäkerhet.
- En kommunikationsplan upprättas, beslutas och implementeras som innebär att anställda aktivt nås av policy och riktlinjer avseende cybersäkerhet. Kommunikationsplanen syftar till att säkerställa att anställda som hanterar kommunens information har kännedom om kommunens policy och riktlinjer avseende cybersäkerhet.

4 Revisionsfrågor

Granskningen har utgått från revisionsfrågan: bedriver Haninge kommun ett tillräckligt och ändamålsenligt cybersäkerhetsarbete? Revisionsfrågan har brutits ner och besvarats enligt tabell 10, 11 och 12.

Tabell 8: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 9: Svar på övergripande revisionsfråga

Övergripande revisionsfråga	Svar	
Bedriver Haninge kommun ett tillräckligt och ändamålsenligt cybersäkerhetsarbete?	Den övergripande bedömningen är att Haninge kommun *delvis* bedriver ett tillräckligt och ändamålsenligt cybersäkerhetsarbete. Svaret grundar sig i nedan besvarade underliggande revisionsfrågor.	

Tabell 10: Svar på underliggande revisionsfråga avseende styrning

Underliggande revisionsfråga	Svar	
Kan *styrningen* av arbetet med cybersäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?	Styrningen av cybersäkerhetsarbetet bedöms vara *delvis* ändamålsenligt. Svaret grundar sig i att det finns ett implementerat ledningssystem för informationssäkerhet samt ett dokumenterat säkerhetsprogram som inkluderar informationssäkerhet. Det finns även en digitaliseringspolicy för IT-säkerhet och tillhörande IT-anvisningar samt en riktlinje för GDPR. Styrningen av cybersäkerhetsarbetet bedöms inte vara fullständigt ändamålsenligt då det saknas riktlinjer och processbeskrivningar för informationssäkerhetsarbetet. Det saknas även en utförlig roll- och ansvarsbeskrivning samt en process för direkt kommunikation av policy och riktlinjer till anställda. Därtill	

	saknas processer för uppföljning/kontroll och kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Se även nedan för underbyggande till bedömningen av styrningen av cybersäkerhetsarbetet.	
▸ Görs riskanalyser avseende cybersäkerhet på ett strukturerat sätt och används dessa för att identifiera åtgärder, baserat på upptäckta risker?	Riskanalyser avseende cybersäkerhet genomförs *inte* på ett strukturerat sätt. Svaret grundar sig i att det finns en modell för risk- och sårbarhetsanalys för åtgärder inför och vid extraordinära händelser. Det genomförs även konsekvensbedömning vid behandling av personuppgifter. Arbetet med riskanalyser bedöms inte vara ändamålsenligt eftersom det inte framgår ur beslutat styrdokument när riskanalys ska genomföras. Det saknas även en formaliserad processbeskrivning av hur riskanalys ska genomföras.	
▸ Finns det en strukturerad metod för att identifiera och skydda kommunens viktigaste informationstillgångar?	Det finns en *delvis* strukturerad metod för att identifiera och skydda kommunens viktigaste informationstillgångar. Svaret grundar sig i att det finns en modell för risk- och sårbarhetsanalys för åtgärder för extraordinära händelser. Enligt modellen ska de processer och system som är kritisk för verksamheten identifieras. Därtill är både intrusion detection system och intrusion prevension system implementerat i nätverksmiljön. Arbetet med att identifiera och skydda kommunens viktigaste informationstillgångar bedöms inte vara fullständigt ändamålsenligt då det saknas en process som säkerställer att driftdokumentation finns på plats för samtliga verksamhetskritiska system. Därtill saknas en process som regelbundet säkerställer att brandväggarnas konfigurationer förblir lämpliga över tid, samt dokumenterad styrning av nätverk och brandväggar.	

▸ Har kommunen tillgång till tillräcklig kompetens? Och finns en tillräcklig egen kompetens?	Kommunen bedöms *delvis* ha tillgång till tillräcklig kompetens och egen kompetens. Svaret grundar sig i det finns en säkerhetsenhet, IT-enhet och dataskyddsombudet som hanterar cybersäkerhetsarbetet. Därmed bedöms kommunen ha tillgång till kompetent personal till cybersäkerhetsområdet men bedömningen är även att det finns behov av ytterligare personal inom området. Eftersom säkerhetsenheten täcker in fler områden än endast informationssäkerhet riskerar kommunens informationssäkerhetsarbete att inte tilldelas den tid och de resurser som krävs för att uppnå ett ändamålsenligt informationssäkerhetsarbete.	

Tabell 11: Svar på underliggande revisionsfråga avseende uppföljning

Underliggande revisionsfråga	Svar	
Är arbetet med att *följa upp* att beslut och styrdokument relaterat till cybersäkerhet efterlevs ändamålsenligt?	Arbetet med att följa upp efterlevnaden av cybersäkerhetsarbetet bedöms vara *delvis* ändamålsenligt. Svaret grundar sig i att det genomförs viss uppföljning av programförändringar samt rapporterade IT-incidenter. Därtill genomförs årlig egenkontroll av dataskyddsarbetet av kommunens nämnder samt en GDPR-rapport av dataskyddsombudet. Uppföljningsarbetet bedöms inte vara helt ändamålsenligt eftersom det saknas en formaliserad process för övergripande uppföljning och kontroll av hur väl anställda inom kommunen efterlever policy och riktlinjer avseende IT- och informationssäkerhet. Det genomförs inte heller någon regelbunden rapportering till kommunstyrelsen av hur cybersäkerhetsarbetet fortlöper.	

Tabell 12: Svar på underliggande revisionsfråga avseende incidenthantering

Underliggande revisionsfråga	Svar	
Är Haninge kommuns *incidenthanteringsprocess* ändamålsenlig?	Kommunens incidenthanteringsprocess bedöms vara *delvis* ändamålsenlig. Svaret grundar sig i att det finns dokumenterade processer avseende IT-incidenter. Det finns även en dokumenterad process för att finna ortorsak och åtgärdsplan samt att IT-incidenter följs upp veckovis. Revisionsfrågan bedöms inte vara uppfylld då det saknas dokumentation som beskriver kommunens hantering av informationssäkerhetsincidenter. Det finns en praktisk process för hantering av informationssäkerhetsincidenter, men denna är inte formaliserad och det sker ingen uppföljning. Se även nedan för underbyggande till bedömningen av kommunens incidenthanteringsprocess.	
▸ Finns en förmåga att öva och utbilda utifrån ett krishanteringsperspektiv?	Förmågan att öva och utbilda utifrån ett krishanteringsperspektiv bedöms *inte* vara ändamålsenlig. Svaret grundar sig i det saknas en formaliserad utbildningsplan med obligatoriska utbildningsmoment avseende cybersäkerhet. Därtill har inte en kontinuitetsplan tagits fram för kommunens samtliga verksamheter. Det sker ingen systematisk och direkt kommunikation till anställda avseende verksamheters kontinuitetsplan och det sker ingen uppföljning eller kontroll för att säkerställa att anställda är medvetna om sin verksamhets kontinuitetsplan.	

5 Slutsatser

Granskningens syfte har varit att bedöma om det finns brister i kommunens interna kontroll avseende cybersäkerheten. Vidare har syftet också varit att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp detta arbete.

Baserat på den analys och granskning som genomförts bedöms Haninge kommun ha en genomsnittlig mognadsgrad på 2,60 vilket är jämbördigt med andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Haninge kommun är mognadsgraden klart lägre än vad EY rekommenderar för en kommun likt Haninge.

EY:s övergripande bedömning är att Haninge kommuns arbete med cybersäkerhet är delvis ändamålsenligt. Bedömningen grundar sig i att det finns ett implementerat ledningssystem för informationssäkerhet samt flertalet övergripande styrdokument, däribland säkerhetsprogram som inkluderar informationssäkerhet, digitaliseringspolicy samt riktlinjer för GDPR. Däremot saknas riktlinjer och processbeskrivningar för informationssäkerhetsarbetet samt en utförlig roll- och ansvarsbeskrivning. Därtill saknas processer för uppföljning/kontroll och kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Bedömningen grundar sig även i att det finns ett behov av en utpekad samordnare för informationssäkerhet samt att det saknas dokumentation som beskriver kommunens hantering av informationssäkerhetsincidenter.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Haninge kommun tillser att:

- En samordnare rekryteras med informationssäkerhet som sitt huvudsakliga ansvarsområde för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.
- Direktivet för informationssäkerhet färdigställs och beslutas för att säkerställa att den övergripande målbilden och ansvarsfördelningen med informationssäkerhet formaliseras och träder i kraft.
- Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.

Stockholm 2022-12-07

_____

Helena Törnqvist, Partner

Bilaga 1: Källförteckning

Dokumentförteckning:

- BCP Kontinuitetsplan Haninge kommun IT-enhetens leveranser
- Beslut om rutin vid backgrundskontroll
- Bilaga 2- Kravspecifikation vid upphandling – tekniska-krav
- DIPA – Haninge Kommun
- Dokumenthanteringsplan_kf_ks
- Draft-it
- Förslag Digitaliceringspolicy efter återremitering av förslag rev it-policy UTKAST
- Förslag rev it-plicy
- Förvaltningsstyrningsmodell – Intranät
- Förvaltningsstyrningsmodell-2020 - Intranät
- Förändringshantering – Intranät
- Förändringshantering för leverantör
- Haninge kommuns policy för styrdokument, ANTAGEN
- Informationsklassning blankett
- Informationssäkerhet – Intranät
- Informationssäkerhet och IT säkerhet Haninge kommun 2022
- Instruktion administration av användarkonto-v1.64
- Intranät – förvaltningsmodell för förvaltning av haninge kommuns it STOD
- IT-anvisningar och riktlinjer
- IT-policy Haninge kommun
- Konsekvensbedömning – Extens grundskola/grundsärskola 2021-11-25
- Kravspecifikation vid upphandlingar – Intranät
- Leveransmodell Change management process
- Leveransmodell Incident management process
- Leveransmodell innehållsförteckning
- Leveransmodell Major Incident management process
- Leveransmodell mötesforum
- Leveransmodell Problem management process
- Leveransmodell Samverkanshandbok
- Leveransmodell Service level management process
- Leveransmodell årshjul mötesforum leverantörsstyrning
- Leveransmodell översikt
- Lösenordsportal – Intranät
- Mall rutiner personuppgiftsbehandling
- Program för säkerhet och riskhantering 2019-2022
- Rapport egenkontroll dataskydd GVN
- Rapportering av säkerhetsincident
- RAS modell som blankett 2.1
- Riktlinjer GDPR
- Riktlinjer- Informationssäkerhet utkast
- Rutin återrappotera GDPR (1)
- Servicedesk (IT och telefon) – Intranät
- Årsrapport dataskyddombudet

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.

Change Advisory Board (CAB): En konstellation av IT- och verksamhetsrepresentanter som stödjer processen avseende förändringar genom att ge råd och fatta beslut.

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.

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.

ITIL V3: ITIL (Information Technology Infrastructure Library) är ett ramverk för att standardisera IT-relaterade aktiviteter. ITIL V3 är en version som även inkluderar strategiska element i syfte att IT bättre ska sammanvävas med verksamheten.

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.

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

Patchning: Tillägg till ett program eller system avsett att rätta till sårbarheter.

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.

Single-sign-on: Autentiseringsschema inom sammansatta datasystem som möjliggör för användare att logga in en gång för att komma åt flera system inom verksamheten.

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

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.

Objektägare: 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.