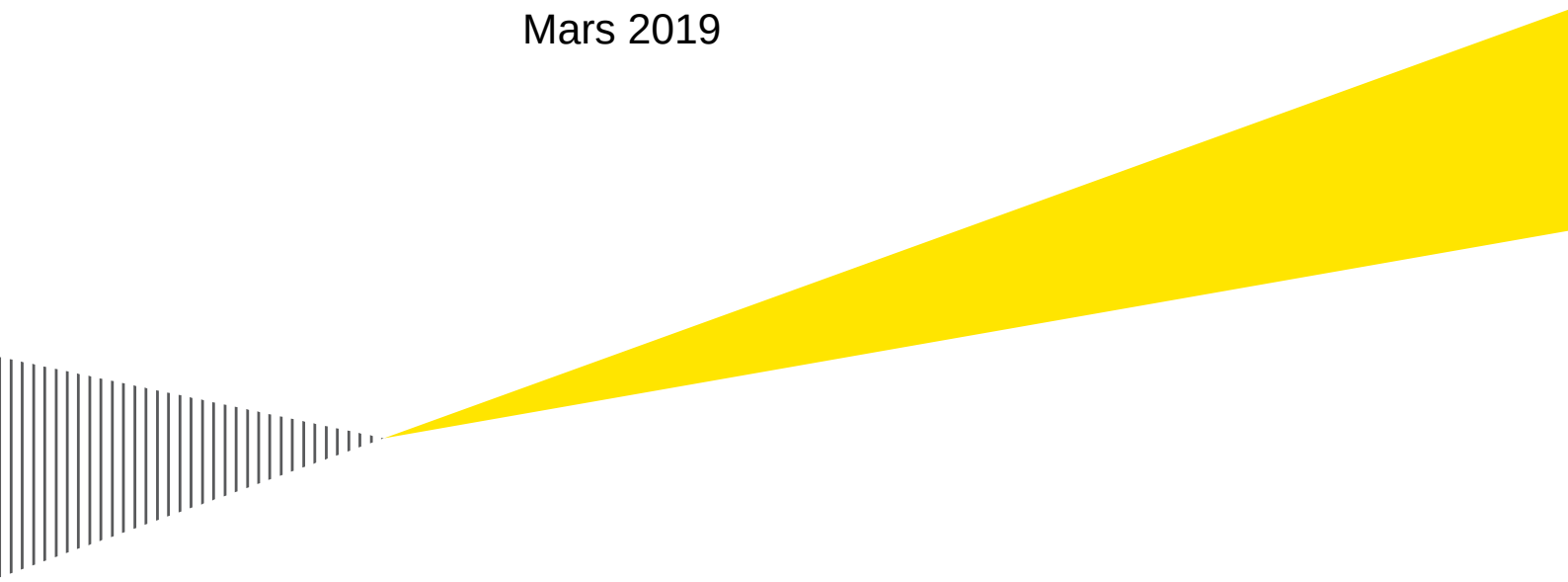
Haninge kommun

Granskning av kommunens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering

Mars 2019



Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Sammanfattning

EY har på uppdrag av Haninge kommuns förtroendevalda revisorer genomfört en granskning av kommunens arbete med informationssäkerhet. Granskningens syfte har varit att ge en övergripande nulägesbild om huruvida Kommunstyrelsen för Haninge kommun har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

Granskningen genomfördes under januari till mars 2019 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad styrdokumentation. Grunden för intervjufrågorna och granskningen som helhet har byggts på EY:s metodstöd *Cybersecurity Program Assessment* (CPA), med fokus på organisation och styrningsrelaterade områden, och *Granskningsprogram Cyber och Informationssäkerhet* (GCI), med fokus på offentlig verksamhet. Både CPA och GCI baseras på erkända ramverk inom informationssäkerhet såsom *ISO27000* och *Myndigheten för Samhällsskydd och Beredskaps* (MSB:s) metodstöd för informationssäkerhet.

Baserat på den utförda granskningen har kommuncentral uppföljning av efterlevnad av informationssäkerhetsrutiner i Haninge kommuns koncernbolag och verksamheter identifierats som kommunens största förbättringsområde. Koncernbolagens informationssäkerhetsarbeten stod vid tiden för granskningen helt utan kommuncentral uppsyn, och inte heller arbetet i kommunens nämnder och förvaltningar följdes upp närmare med formaliserade kontroller och rutiner för säkerställande av efterlevnad.

Mognadsnivån i kommunens arbete med informationssäkerhet bedöms annars generellt vara god. Kommunen har etablerat relevanta styrdokument med tillhörande användarinstruktioner, inklusive en väl fungerande incidenthanteringsprocess som är utformad enligt god praxis. Kommunen har även definierat och utsett dedikerade informationssäkerhetsresurser både i den kommuncentrala Kommunstyrelseförvaltningen och i verksamheterna. Med bakgrund i detta bedöms Haninge kommun ha goda förutsättningar att bedriva ett ändamålsenligt arbete med informationssäkerhet på både kort och lång sikt.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Innehållsförteckning

Bildförteckning

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. Bakgrund

Haninge kommun, dess nämnder, förvaltningar (nämnder och förvaltningar hänvisas hädanefter till samlingsbegreppet ”kommunens verksamheter”) och koncernbolag hanterar stora mängder digital information. Hantering av digital information medför möjligheter i form av effektivare daglig verksamhet, uppföljning och utökad service till medborgarna, samtidigt som risker uppstår om informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrningen och arbetet bedrivs på ett sådant sätt att informationen hålls konfidentiell och är riktig, tillgänglig för rätt personer och spårbar.

Med bakgrund i ovan genomförde EY på uppdrag av Haninge kommuns förtroendevalda revisorer under januari till mars 2019 en granskning av kommunens arbete med informationssäkerhet.

1.2. Syfte och revisionsfrågor

Syftet med granskningen var att ge en övergripande nulägesanalys om huruvida Kommunstyrelsen för Haninge kommun har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt. Granskningen syftar att ge svar på tre revisionsfrågor:

- Hur ändamålsenlig är styrningen av arbetet med informationssäkerhet gentemot LIS-ramverket (i enlighet med MSB:s metodstöd och ISO27000) för de behov kommunens verksamhet har?
- Hur ändamålsenligt är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs?
- Har Haninge kommun en ändamålsenlig incidenthanteringsprocess?

1.3. Avgränsningar

De iakttagelser som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom inspektion av erhållen dokumentation, såsom styrningsdokument, riktlinjer och planer. Haninge kommuns nämnder, förvaltningar och koncernbolag har inte granskats mer än utifrån den information som har erhållits från kommunförvaltningens centrala informationssäkerhetsresurser. Ingen teknisk granskning eller analys har genomförts. Vidare har inga stickprov på efterlevnad tagits.

1.4. Metod och genomförande

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete samt genomgång av relevant styrdokumentation (se *Sektion 8. Bilaga 2: Källförteckning*). Granskningen är utförd mot god praxis inom informations- och IT-säkerhetsområdet och bygger på EY:s metodstöd *Cybersecurity Program Assessment* (CPA), med fokus på organisation och styrningsrelaterade områden, och *Granskningsprogram Cyber och Informationssäkerhet* (GCI), med fokus på offentlig verksamhet. Både CPA och GCI baseras på erkända ramverk inom informationssäkerhet såsom *ISO27000* och *Myndigheten för Samhällsskydd och Beredskaps* (MSB:s) metodstöd för informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

De intervjuade har beretts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Granskningen har även kvalitetssäkrats av EY:s verksamhetsrevisorer och presenterats för Haninge kommuns förtroendevalda revisorer.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2. Strategi, styrning och organisation

2.1. Styrdokument

Arbetet med informationssäkerhet i Haninge kommun har under de senaste tre åren underordnats den informationssäkerhetspolicy som fastslogs och beslutades av Haninge kommuns kommunfullmäktige den 21 mars 2016. Informationssäkerhetspolicyn stipulerar att den är att betrakta som giltig för alla nämnder och dess förvaltningar inom Haninges kommunkoncern och skall beaktas vid all hantering av informationstillgångar. Policyn beskriver övergripande strategiska målområden, bland annat rörande användares kunskapsnivåer kring ämnet, upprättande av förteckningar över informationstillgångar och genomförande av informationsklassningar. Policyn innehåller även ansvar och roller samt krav på uppföljning inom ramen för kommunens informationssäkerhetsarbete. Ett antal användaranvisningar har också upprättats som underordnade stöd till kommunens policy (se sektion *3.1 Användarinstruktioner*).
Haninge kommuns koncernbolag innefattas inte av informationssäkerhetspolicyn utan är ansvariga för sina egna styrmodeller för informationssäkerhet.

2.2. Ansvarsfördelning och organisation

Haninge kommuns Kommunstyrelse är ytterst ansvarig för säkerställandet av ändamålsenlig informationssäkerhet för hela kommunkoncernens digitala informationstillgångar. En organisationsstruktur som stöder detta finns på plats, dock med utelämnande av kommunens koncernbolag. Bolagen är sina egna informationsägare och bedriver egna informationssäkerhetsarbeten, men centrala insynsrutiner saknas och de har inga krav på återrapportering till Kommunstyrelseförvaltningen kring hur arbetet genomförs eller fortskrider.

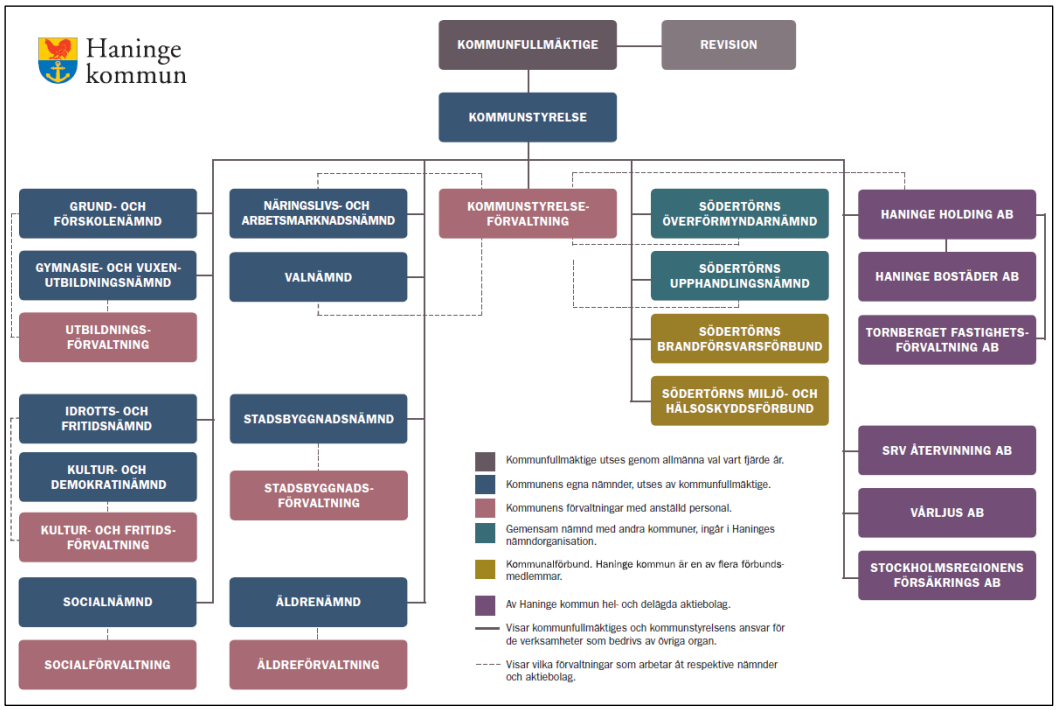


Bild 1: Organisationskarta - Haninge kommun[1]

[1] https://www.haninge.se/kommun-och-politik/kommunens-organisation/, 2019-02-04

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

För Haninge kommuns nämnder och förvaltningar är Kommunstyrelsen ansvarig för att utveckla och överse strategiska målområden inom informationssäkerhetsarbetet. Dessa delegeras sedan till en kanslienhet på Kommunstyrelseförvaltningsnivå för verkställande. I kansliet ingår bland annat kommunjurister och dataskyddsombud, och enheten arbetar med att definiera regler, riktlinjer och anvisningar för kommunens verksamheter.

Den kommuncentrala enheten Digital Utveckling ansvarar för IT-säkerheten (se sektion *7. Bilaga 1: Definitioner*) inom Haninge kommuns informationssäkerhetsarbete. Detta innebär att enheten stöder verksamheterna utifrån de säkerhetskrav som respektive verksamhet har, exempelvis baserat på lagstadgade krav eller utfall från genomförda informationsklassningar och riskanalyser.

Liksom koncernbolagen är Haninge kommuns enskilda nämnder och förvaltningar sina egna informationsägare. Detta betyder att de är ansvariga för sin egen informationshantering och för att informationssäkerhetsarbetet inom verksamheten bedrivs på ett ändamålsenligt sätt och i enlighet med anvisningar från Kommunstyrelseförvaltningen. Verksamheternas respektive förvaltningschef är ytterst ansvarig för detta och iklär sig ofta rollen som objektsägare inom verksamheten. Haninge kommun definierar ett objekt som ett system, applikation, funktion eller tjänst, och objektsägaren har således övergripande ansvar för objektet och dess användning. Objektsägaren skall också utse en förvaltningsledare och minst en objektsspecialist per objekt. Förvaltningsledarens uppgift är att se till att objektet i fråga förvaltas ändamålsenligt, medan objektsspecialisterna stöder förvaltningsledaren i det operationella arbetet för objekten och ser till att funktionalitet upprätthålls och aktiviteter utförs.

I tillägg har rollen som IT-strateg definierats för samtliga av Haninge kommuns förvaltningar. IT-strategernas ansvar är att fånga upp verksamheternas IT-relaterade behov, innefattandes informationssäkerhet, och omsätta dessa till korrelerande kravställningar mot Digital Utveckling. IT-strategerna fungerar tillsammans med förvaltningsledarna som länken mellan verksamheterna och de centrala kansli- och Digital Utvecklingsenheterna i Kommunstyrelseförvaltningen.

I genomförda intervjuer har det framkommit att Haninge kommuns verksamheter till stor del utför arbetet med informationssäkerhet självständigt och med begränsad uppföljning från Kommunstyrelseförvaltningen. Exempel på områden som inte brukar följas upp regelbundet och aktivt inkluderar genomförande av informationsklassning och hantering av avtal för externa leverantörer (se sektion *3.4 Informationsklassning* respektive *2.3 Externa leverantörer och hantering av leverantörsavtal*). Däremot uppgavs det att den informella samverkan mellan verksamheternas IT-strateger och förvaltningsledare gentemot kansliet och Digital Utveckling är relativt god. Representanter från kansliet och Digital Utveckling bjuds ofta in att medverka vid förvaltningsledarnas möten, där förutsättningar för informationssäkerhetsefterlevnad regelbundet är diskussionsunderlag.

2.3. Externa leverantörer och hantering av leverantörsavtal

Alla upphandlingar av centrala och kommunövergripande IT-system i Haninge kommun underordnar sig Lagen om Offentlig Upphandling och går via upphandlingsenheten som svarar till Kommunstyrelseförvaltningen. Inga specifika upphandlings- och leverantörsavtal för just informationssäkerhet har definierats, men krav och instruktioner för hur leverantörerna skall handha information de har tillgång till skall vara del av de avtal som upphandlingsenheten tar fram.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Hela Haninge kommuns nuvarande IT-infrastruktur, inklusive nätverk, drivs och underhålls av ett fåtal externa leverantörer. En samverkanshandbok har definierats av Kommunstyrelseförvaltningen tillsammans med representanter från de externa leverantörerna. Handboken beskriver de samverkansformer som Haninge kommun och leverantörerna skall förhålla sig till för att styra och följa upp på frågor och ärenden kring avtal och tjänsteleverans. Handboken innehåller bland annat nyckelroller både hos kommunen och leverantörerna, kontaktuppgifter, eskaleringsmatriser, samverkansforum och en sammanställning av tillgänglighetskrav per leverans och incident. Ett specifikt, taktiskt leverantörsforum på månadsbasis har definierats för att säkerställa att det sker en gemensam översyn av status för leverans, eskaleringar, samverkan och proaktivitet i förhållande till leverantörsavtal.

För verksamhetsspecifika IT-system har en utvecklingsprocess definierats. Utvecklingsprocessen beskriver de steg som Haninge kommuns verksamheter skall ta vid upphandlingar, införanden och avvecklingar av objekt i verksamheterna. Som del av processen skall Digital Utveckling involveras i flertalet steg för centralt och standardiserat säkerställande av kvalitet, säkerhetskrav och förvaltning. Bland annat ställs krav på att varje IT-system skall kompletteras av en systemspecifik förvaltningsplan, som delvis baseras på att klassning av systemets informationstillgångar utförs (se sektion *3.4 Informationsklassning* och *3.5 Driftdokumentation och kontinuitetsplanering*). Dock är verksamheterna ansvariga för att utforma och underhålla sina egna leverantörsavtal och ingen kommuncentral uppföljning av avtalens utformning och efterlevnad genomförs.

Koncernbolagen delar viss IT-infrastruktur med övriga kommunen, exempelvis nätverk, men majoriteten av deras IT-miljöer är bolagsspecifika och följs därmed inte upp närmare av Kommunstyrelseförvaltningen.

2.4. Personal och utbildning

I genomförda intervjuer har det framförts att Kommunstyrelseförvaltningen vid perioden för denna granskning (januari till mars 2019) är tillfredsställda med både antalet resurser i Haninge kommuns informationssäkerhetsarbete och deras kompetensnivå. Rollerna som förvaltningsledare och IT-strateger finns tillsatta i samtliga verksamheter och driver informationssäkerhetsagendan utifrån Kommunstyrelseförvaltningens övergripande bestämmelser. Den i intervjuerna uttalade målbilden är snarare att bredda och öka kunskapsnivån om informationssäkerhet närmare informationshanteringen i verksamheterna än att tillsätta centrala resurser för arbete med styrning.

I samband med införandet av den kommunövergripande informationssäkerhetspolicyn i mars 2016 genomfördes ett antal frivilliga utbildningsinitiativ rörande informationssäkerhet för kommunverksamheternas anställda. Utbildningarna levererades digitalt som en koordinerad serie bestående av 18 ”nanoutbildningar” på ca två till tre minuter var. Statistik angående deltagarantal finns tillgängligt men ingen uppföljning på utbildningarna har gjorts och ingen formaliserad utbildningsrutin eller plan har definierats. Även en nischad utbildning i samma korta serieformat genomfördes för personuppgiftshantering i samband med att dataskyddsförordningen (GDPR) effektuerades i maj 2018. Utbildningarna var ursprungligen tillgängliga på Haninge kommuns intranät men har nu ersatts av dokument som sammanfattar innehållet i utbildningarna. Deltagande i informationssäkerhets- och dataskyddsförordningsutbildningarna för nyanställda är inte obligatoriskt. För tillfället täcks inte informationssäkerhet eller personuppgiftshantering i den introduktionsinformation som nyanställda får ta del av vid anställning.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2.5. Styrning av åtkomsthantering

Vid uppkoppling mot Haninge kommuns nätverk tillämpas enkel inloggning (single sign-on) för en majoritet av kommunens förvaltningsobjekt via en central identitetshanterings- och inloggningsportal. Detta gäller emellertid inte då användaren vid inloggning inte befinner sig på kommunens nätverk utan loggar in via internet, och flertalet system kan inte tillgås alls utan uppkoppling mot kommunens nätverk.

Haninge kommuns användares konton fylls i automatiskt vid åtkomsttilldelning baserat på information i kommunens personalsystem. Innan användarna kan börja använda kontona krävs dock godkännande av användarnas ansvariga chef eller tillförordnad. Denna skall kontrollera att informationen från personalsystemet är korrekt och markerar vilka objekt som den berörda användaren behöver åtkomst till. För åtkomst till objekt som inte är listade i portalen och därmed inte omfattas av enkel inloggning, beställer ansvarig chef den eftersökta åtkomsten av Haninge kommuns Service Desk, alternativt kontaktar ansvarig förvaltningsledare eller objektsspecialist. Service Desk utvärderar beställningen innan åtkomsten till användarna tilldelas. Borttagning av åtkomster till följd av exempelvis avslutad anställning utförs enligt samma rutiner som vid tilldelning.

Inga rutiner för säkerställande av ändamålsenlig ansvarsfördelning i användares åtkomstuppsättningar har definierats. Däremot innehåller flertalet IT-system, bland annat kommunens ekonomisystem, logiska regelbestämmelser för att undvika att konflikterande behörigheter tilldelas samma användare. Upprättandet och underhållet av dessa regelbestämmelser faller under objektsspecialisternas ansvar.

Tilldelning av användarkonton med priviligierade behörigheter genomförs via direkt kontakt med berörd objektsspecialist. Inga specifika anvisningar för hur objektsspecialisterna skall förhålla sig till tilldelningen av dessa behörigheter finns definierade. Användarkonton med priviligierade behörigheter finns främst hos Haninge kommuns driftsleverantörer. Dessa konton, bland annat domänadministratörer, granskas årligen i periodiska genomgångar som utförs av respektive objekts förvaltningsledare. Genomgångarna är dock inte formaliserade, och för genomgångar av vanliga användarkonton saknas standardiserade rutiner. Faktiskt utförande av periodiska genomgångar sker ofta spontant i samband med att informationstillgångar klassas eller vid förändringar i IT-miljön.

Lämplig lösenordskomplexitet för användarkonton säkerställs med förutbestämda regler mot identitetshanteringsportalen, dock utan krav på bytesfrekvens. Tvåfaktorsautentisering är implementerat för en del objekt som i och med genomförd informationsklassning har identifierats innehålla information av känslig karaktär, vilket bland annat inkluderar Äldreförvaltningens verksamhetssystem.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Operationella rutiner

3.1. Användarinstruktioner

På Haninge kommuns intranät har ett antal användarinstruktioner definierats. Anvisningarna omfattar övergripande förhållningssätt när det kommer till införande av molntjänster och IT-stöd, privata användningsrutiner av kommunens IT och telefoni, användarkontohantering, behandling av känslig information i e-post samt lagringsrutiner. Samtliga användarinstruktioner har tagits fram på Kommunstyrelseförvaltningsnivå och är tillgängliga för samtliga av kommunkoncernens medarbetare. Dock kommuniceras instruktionerna inte aktivt ut till verksamheterna utan förutsätter att användarna själva lokaliserar informationen.

3.2. Incidenthantering

Haninge kommun har inte definierat särskilda rutiner för informationssäkerhetsrelaterade incidenter, utan dessa omfattas av kommunens övergripande incidentprocess. Processen har tagits fram i enlighet med IT-tjänsteprinciperna ITIL v3 (Information Technology Infrastructure Library). Då driften av Haninge kommuns IT-miljö är utlokaliserad till externa leverantörer har kommunens SIAM-funktion (Service Integration & Management), som är en del av Service Desk, en nyckelroll i att koordinera hanteringen av incidenter i samförstånd med externa leverantörer. SIAM-funktionen rapporterar även incidenthanteringsförfarandet till Digital Utveckling.

I och med IT-driftutlokaliseringen underströks det i genomförda intervjuer att de flesta incidenter först identifieras i de externa leverantörernas monitoreringsverktyg. Om kommunens egna anställda misstänker att intrång eller andra störningar är i skeende skall detta rapporteras direkt till Service Desk, vilket finns beskrivet på kommunens intranät. Service Desk involverar sedan relevanta intressenter och eskalerar om nödvändigt ärendet. Ett särskilt processflöde för kritiska incidenter (major incident process) har definierats som komplement till incidentprocessen och skall initieras av Service Desk om den identifierade incidenten registreras med en kritisk prioriteringsnivå.

Uppföljning av kommunens incidenthantering görs i definierade operativa forum. Kritiska incidenter genererar också en incidentrapport som beskriver vilken typ av incident som drabbade kommunen, dess påverkan och hur den löstes. Inga dokumenterade och bindande krav finns på att rapportera incidenter till Kommunstyrelsen, även om särskilt kritiska incidenter rapporteras till Kommunstyrelsen informellt. Under perioder när särskilda informationssäkerhetsrelaterade hot har identifierats, exempelvis när ett stort antal nätfiskeförsök spreds via e-post bland Haninge kommuns användare, skickades information ut från Kommunstyrelseförvaltningen till användarna att agera varsamt och att rapportera misstänksam aktivitet.

Införandet av dataskyddsförordningen medförde även att Haninge kommun, som tillägg till incidentprocessen, har definierat en särskild lathund för hur kommunens användare skall rapportera incidenter relaterade till personuppgifter. Lathunden kompletteras av mer utförliga anvisningar tillgängliga på intranätet som ägs och underhålls av Haninge kommuns dataskyddsombud.

3.3. Programförändringsrutiner

Liksom för Haninge kommuns incidentprocess har en programförändringsprocess definierats i enlighet med ITIL v3. Haninge kommun utför ingen egen utveckling av programvara men

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

har genom processen formaliserat kravställningsrutiner av programförändringar gentemot sina externa leverantörer och utvecklare. Förvaltningsledare och objektsspecialister är huvudansvariga för att framföra förändringsbeställningar till kommunens Service Desk, som agerar som uppsamlingspunkt för samtliga förändringsbeställningar i kommunen. Förändringsbeställningar kan också initieras från de externa leverantörerna, exempelvis i form av uppgraderingar eller nödvändiga patchar. Förändringsbeställningarna gås sedan igenom och diskuteras i regelbundna förändringsråd en gång i veckan med utfallet att beställningarna antingen godkänns eller avslås.

För att beställningar skall godkännas skall risken av att utföra förändringarna kartläggas. I dessa riskanalyser finns utrymme att lyfta särskilda informationssäkerhetsrelaterade risker, men i övrigt finns inga krav på att utvärdera programförändringar från ett informationssäkerhetsperspektiv. Programförändringar utförs sedan av externa leverantörers tekniker under överenskomna underhållstidpunkter.

I och med att Haninge kommuns koncernbolag har sina egna IT-miljöer omfattar inte den definierade programförändringsprocessen bolagen utan är begränsad till de objekt som förvaltas av Kommunstyrelseförvaltningen genom Digital Utveckling.

3.4. Informationsklassning

Piloter har genomförts inom alla Haninge kommuns förvaltningar för att identifiera de förvaltningsobjekt som anses innehålla informationstillgångar av skyddsvärde. Piloterna omfattade inte alla verksamheternas objekt men resulterade i att informationen i de största och mest använda systemen inom verksamheterna klassades. Klassningarna genomfördes med avstamp i en egen, övergripande informationsklassningsmodell, där utfallet var en färgkod motsvarande en prioriteringsnivå. För system som innehöll information med prioriteringsfärgkoderna röd och gul var fullständig klassning i SKL:s KLASSA-verktyg nödvändig, medan kommunens egna klassning ansågs vara tillräcklig för system med information som erhöll en grön prioriteringsnivå. Haninge kommuns koncernbolag har ej omfattats av informationsklassningspiloterna men intresse finns hos ett av bolagen att ta efter klassningsmodellen.

Ägarskap för genomförande och uppföljning av informationsklassningarnas utfall ligger hos respektive objekts objektsspecialist, under översikt av objektets förvaltningsledare. Vikten av att utföra informationsklassningar för kommunens förvaltningsobjekt lyftes i möte av representanter från Kommunstyrelseförvaltningen, då dessa till stor del spelar in på de förvaltningsplaner som definieras för varje objekt. Förvaltningsplanen är respektive objekts styrande dokument, och beskriver vilka aktiviteter och åtaganden som skall göras för objektet baserat på de informationstillgångar och komponenter som objektet omfattar (se sektion *3.5 Driftdokumentation och kontinuitetsplanering*).

3.5. Driftdokumentation och kontinuitetsplanering

Haninge kommun har tagit fram en förvaltningsmodell som ett verktyg för att styra arbetet med både centrala och verksamhetsspecifika förvaltningsobjekt. Förvaltningsmodellen ägs och följs upp av Digital Utveckling och syftar till att standardisera förvaltningen av objekt när det kommer till bland annat arbetsformer och roller. Koncernbolagens objekt och IT-miljöer omfattas inte av förvaltningsmodellen.

Haninge kommuns förvaltningsmodell ställer krav på att förvaltningen av varje enskilt objekt skall styras av en förvaltningsplan. Förvaltningsplanen definieras av respektive objekts

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

förvaltningsledare i samråd med objektsspecialister enligt en standardiserad mall från Digital Utveckling. Mallen fastställer att de system, verksamhetskomponenter och informationstillgångar som finns inom objektet kartläggs, inklusive beroenden mot andra objekt. Externa leverantörer och deras avtal skall också framgå, liksom vilka resurser som innehar de olika rollerna i objektets förvaltning.

Planerna beskriver även vilka arbets- och beslutsforum som finns etablerade i arbetet med objekten samt vilken budget som finns avsatt. Förvaltningsplanen skall också innehålla beskrivning och länk till de bilagor som tillhör förvaltningsobjektet, såsom systemdokumentation, systemkarta, säkerhetsklassning och informationsklassning.

Förvaltningsplanerna innehåller inga konkreta krav på eller hänvisningar till kontinuitetsplanering eller definiering av krishanteringsplaner för förvaltningsobjekten. Krav på kontinuitetsplanering ställs istället via informationsklassningsrutinerna, där objekt som via SKL:s KLASSA-verktyg har erhållit kritiska skyddsvärden även skall kontinuitetsplaneras för. Det faktiska genomförandet av kontinuitetsplanering av objektsförvaltningsorganisationerna följs dock inte upp ytterligare av Kommunstyrelseförvaltningen eller Digital Utveckling. Som tillägg finns det även möjlighet att beställa utökad redundans och tillgänglighet för vissa system under vissa perioder från de externa leverantörerna, exempelvis för skolans betygssystem som måste fungera under maj månad varje år.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4. Dataskyddsförordningen och personuppgiftshantering

4.1. Arbetet med dataskyddsförordningen

Haninge kommuns arbete för att förbereda inför dataskyddsförordningens införande påbörjades i november 2017. Arbetet resulterade i att rollen som dataskyddsombud tillsattes på Kommunstyrelseförvaltningsnivå med syfte att driva det kontinuerliga personuppgiftsarbetet centralt och i kommunens verksamheter och koncernbolag. Som stöd till dataskyddsombudet har varje nämnd och korrelerande förvaltning utsett en dataskyddskoordinator, medan koncernbolagen har utsett dataskyddssamordnare. Dataskyddskoordinatorerna och dataskyddssamordnarna driver verksamheternas och koncernbolagens personuppgiftshantering och rapporterar till dataskyddsombudet.

För att kartlägga vilka personuppgifter som hanteras inom verksamheternas förvaltningsobjekt har varje dataskyddskoordinator ansvaret för att tillse att respektive förvaltningschef upprättar verksamhetsspecifika registerförteckningar. Registerförteckningarna skall innehålla all personuppgiftsbehandling som utförs inom respektive objekt och verksamhet, och genereras baserat på 33 personuppgiftsrelaterade frågor. Vid tiden för denna granskning (mars 2019) hade ungefär 180 förteckningar för olika förvaltningsobjekt i kommunens verksamheter upprättats och gjorts tillgängliga för dataskyddsombudet för kontroll och granskning.

Under 2018 genomfördes en utbildning i miniserieformat för kommunens anställda angående implikationerna av dataskyddsförordningen och de ökade kraven kring personuppgiftshantering. Denna har inte gjorts tillgänglig på intranätet för repetition eller uppföljning, men har sammanfattats som ett läsbart Microsoft Word-dokument på intranätet.

Dataskyddsförordningsarbetet har även resulterat i att rutiner för rättighetsutövning har upprättats och att blanketter för registerutdrag gjorts tillgängliga för kommunens medborgare att ladda ned.

4.2. Personuppgifter i molntjänster

Ett antal molnbaserade tjänster hanterar personuppgifter för Haninge kommun, bland annat det vård- och omsorgssystem som finns upprättat inom kommunens Äldreförvaltning. För upphandling av nya molntjänster ställer Digital Utveckling för tillfället krav på att molntjänsternas serverhallar måste vara lokaliserade inom EU:s gränser, men har uttryckt att detta skall justeras till inom Sveriges gränser framöver.

Personuppgiftsbiträdesavtal (PUB-avtal) med krav på säker personuppgiftshantering och sekretess har sedan dataskyddsförordningsens införande definierats för alla upphandlade externa utförare och leverantörer av molntjänster.

4.3. Personuppgiftsincidenter

Under 2018 registrerades sammanlagt fem incidenter av personuppgiftskaraktär, främst rörande förlorad IT-utrustning såsom mobiltelefoner eller persondatorer. Två av de fem personuppgiftsincidenterna rapporterades via dataskyddsombudet vidare till datainspektionen. Instruktioner har definierats på Haninge kommuns intranät för hur kommunens användare skall rapportera incidenter relaterade till personuppgifter.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5. Iakttagelser och rekommendationer

Nedan följer en beskrivning av de iakttagelser och risker som har identifierats under granskningens utförande, tillsammans med rekommendationer och förslag på åtgärder riktat till Haninge kommuns Kommunstyrelse:

5.1 Avsaknad av ändamålsenlig uppföljning av koncernbolagens informationssäkerhetsarbeten	
Iakttagelse	Kommunstyrelsen har inte tillsett att godtagbar uppsikt, i enlighet med Kommunallagen 6 kap. 1 §, i koncernbolagens informationssäkerhetsarbeten kan säkerställas då formella rapporteringskrav till Kommunstyrelseförvaltningen ej har fastställts. Kommunstyrelseförvaltningen följer inte upp på hur koncernbolagen arbetar med informationssäkerhet, varken som helhet eller för viktiga enskilda initiativ såsom informationsklassning och objektsförvaltning. Insikt saknas även i hur koncernbolagen hanterar information som delas över de gemensamma nätverk som kommunen och koncernbolagen använder.
Risk	Avsaknad av kontroll och insikt i koncernbolagens informationssäkerhetsarbete medför risk för att eventuella brister som står under Kommunstyrelsens uppsiktsplikt inte upptäcks och att mognadsnivån i informationssäkerhetsarbetet mellan kommunen och koncernbolag skiljer sig. Detta kan exempelvis leda till att konfidentiell och känslig information läcks, att information är tillgänglig för individer som inte bör ha åtkomst, att information förvrängs eller att spårbarhet inte är möjlig.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att koncernbolagens arbete med informationssäkerhet aktivt följs upp och ökar kraven på återrapportering till Kommunstyrelseförvaltningen, alternativt även inkorporerar bolagen i den övergripande styrmodellen för informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.2 Bristfällig uppföljning av efterlevnad av informationssäkerhetsrutiner i kommunens nämnder och förvaltningar	
Iakttagelse	Kommunstyrelsen har inte tillsett att det finns formaliserade kontroller och rutiner för Kommunstyrelseförvaltningen att följa upp på arbetet med informationssäkerhet i Haninge kommuns nämnder och förvaltningar. Detsamma gäller uppföljningen av efterlevnad av kommunövergripande anvisningar för informationssäkerhetsresurserna i Haninge kommuns verksamheter (objektsägare, förvaltningsledare, objektsspecialister och IT-strateger), vilka bland annat inkluderar rutinerna för informationsklassning, förvaltningsplaner och leverantörsavtal (se iakttagelse 5.3).
Risk	Begränsad uppföljning av verksamheternas informationssäkerhetsarbeten medför risk för att nämndernas och förvaltningarnas dagliga informationshantering avviker från sättet som Kommunstyrelseförvaltningen anvisar och tror att arbetet bedrivs på. Detta kan leda till bristande kontroll i form av ojämn mognadsnivå mellan verksamheterna och att riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som hanteras ej säkerställs.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att adekvata kontroller och rutiner för uppföljning och efterlevnadsutbyte mellan Kommunstyrelseförvaltningen och verksamheterna definieras.

5.3 Brist på uppföljning av utformning och efterlevnad av nämndernas och förvaltningarnas leverantörsavtal	
Iakttagelse	Kommunstyrelsen har inte tillsett att central uppföljning av hur Haninge kommuns nämnder och förvaltningar utformar och underhåller sina avtal med externa leverantörer för att garantera att säker informationshantering efterlevs.
Risk	Brist på uppföljning av leverantörsavtal i enlighet med kommunens upphandlingsprocess medför risk för att externa leverantörer inte hanterar kommunens information ändamålsenligt och i enlighet med god praxis. Detta kan leda till att information hanterad av leverantörer inte har adekvat tekniskt skydd vilket kan riskera eventuella intrång. Vidare kan detta innebära att information inte är tillgänglig för rätt personer, att spårbarhet inte är möjlig och att information förvrängs eller läcks.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att verksamhetsspecifika leverantörsavtal samlas in för granskning och kvalitetssäkring gentemot upphandlingsprocessen med regelbunden frekvens, alternativt måste godkännas av den centrala upphandlingsenheten innan de externa avtalen görs gällande.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.4 Begränsade utbildningar rörande informationssäkerhet och brist på uppföljning av deltagande	
Iakttagelse	Kommunstyrelsen har inte tillsett att det finns obligatoriska och regelbundet återkommande utbildningar inom informationssäkerhet för Haninge kommuns användare. Ingen uppföljning av deltagarantal i tidigare, frivilliga utbildningsinsatser har genomförts. Utbildningarna är ej fortsatt tillgängliga för användarna och i den introduktionsinformation som nyanställda får ta del av vid anställning saknas anvisningar rörande säker informations- och personuppgiftshantering.
Risk	Avsaknad av obligatoriska och regelbundet återkommande utbildningsinsatser rörande informationssäkerhet medför risk för att kommunens användare besitter otillräcklig kunskap för att på daglig basis hantera kommunens information på ett ändamålsenligt och säkert sätt.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att en utbildningsplan för informationssäkerhet formaliseras. Denna bör innefatta genomförande av obligatoriska och regelbundna utbildningar inom informationssäkerhet med uppföljning av deltagarantal och som är tillgängligt på Haninge kommuns intranät. Det redan framtagna ”nanoutbildningsinitiativet” rörande informationssäkerhet rekommenderas att inkluderas i introduktionsinformationen för nyanställda användare.

5.5 Avsaknad av kommunövergripande instruktioner för säkerställande av periodiska genomgångar och ändamålsenlig ansvarsfördelning	
Iakttagelse	Kommunstyrelsen har inte tillsett att kommunövergripande instruktioner för periodiska genomgångar av användare med tillgång till Haninge kommuns olika förvaltningsobjekt har definierats, och genomgångar utförs idag informellt och med begränsad utfallsdokumentation. Även funktionalitet och rutiner för att säkerställa ändamålsenlig ansvarsfördelning i användares åtkomstuppsättningar saknas.
Risk	Avsaknad av säkerställande av periodiska genomgångar och ändamålsenlig ansvarsfördelning medför risk för att olämpliga användare, både interna och externa, har åtkomst till förvaltningsobjekt, servrar och databaser samt att användares åtkomstuppsättningar innehåller konflikterande behörighetsrättigheter. Detta kan i sin tur leda till att konfidentiell och känslig information läcks eller förvrängs.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att kommunövergripande kontroller utformas för standardisering av genomförande av periodiska genomgångar. Kommunstyrelsen rekommenderas också tillse att förteckningar eller matriser skapas kring vilka behörigheter som inte är lämpliga att kombinera inom och mellan kritiska förvaltningsobjekt.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.6 Bristfällig spårbarhet i åtkomsttilldelningen av priviligierade behörigheter	
Iakttagelse	Kommunstyrelsen har inte tillsett att åtkomsttilldelning av priviligierade behörigheter till Haninge kommuns förvaltningsobjekt inte genomförs via direkt kontakt med relevant objektsspecialist utan formaliserade krav på dokumenterade behörighetsbeställningar. Inga specifika anvisningar för hur objektsspecialisterna skall hantera tilldelningen av dessa behörigheter finns definierade.
Risk	Bristfällig spårbarhet i hur åtkomst till priviligierade behörigheter tilldelas och begränsade anvisningar för hur tilldelningen bör gå tillväga ökar risken för att olämpliga användare, både interna och externa, har åtkomst till förvaltningsobjekt, servrar och databaser.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att tilldelningen av priviligierade behörigheter till kommunens förvaltningsobjekt följer en definierad behörighetsprocess eller anvisningar.

5.7 Passiv lagring av informationssäkerhetspolicy och relaterade anvisningar	
Iakttagelse	Haninge kommuns informationssäkerhetspolicy och användaranvisningar lagras passivt på kommunens intranät och förutsätter att användare avsiktligt letar upp den information de eftersöker.
Risk	Brist på aktiv kommunikation av policys, anvisningar och instruktioner gällande informationssäkerhet medför risk för att kommunens användare besitter otillräcklig kunskap för att på daglig basis hantera kommunens information på ett ändamålsenligt och säkert sätt.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till kommunens användare med en bestämd frekvens. Särskilt fokus bör läggas på anvisningar som är applicerbara i dagligt arbete, såsom privata användningsrutiner av kommunens IT och telefoni, användarkontohantering, behandling av känslig information i e-post samt lagringsrutiner. Nyanställda rekommenderas även få tillgång till denna dokumentation vid tidpunkt för påbörjad nyanställning.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.8 Brist på kommunövergripande kontinuitetsplanering och uppföljning av objektsspecifika kontinuitetsplaner	
Iakttagelse	Kommunstyrelsen har inte tillsett att övergripande rutiner har definierats kring hur Kommunstyrelseförvaltningen, nämnderna, förvaltningarna och koncernbolagen ska samordna och verka som helhet i händelse av katastrofer som hotar hela kommunen. Viss kontinuitetsplanering uppges ha utförts för enskilda förvaltningsobjekt med information som har klassats som skyddsvärd, dock utan central uppföljning av Kommunstyrelseförvaltningen eller Digital Utveckling för säkerställande av kvalitet, standardisering och testningsutförande.
Risk	Avsaknad av eller bristfälliga kontinuitetsplaner medför risk för att Haninge kommun misslyckas att ändamålsenligt hantera katastrofer som kan orsaka verksamhets- eller samhällskritiska förluster av informationstillgångar.
Rekommendation	EY rekommenderar att Kommunstyrelsen tillser att kontinuitetsplanering genomförs på koncernövergripande nivå i samråd med lämpliga representanter från verksamheterna och koncernbolagen. Kommunstyrelsen rekommenderas också att tillse att tydliga anvisningar definieras för när objektsspecifik kontinuitetsplanering skall bedömas nödvändigt, förslagsvis som del i mallen för förvaltningsplanen. Samtliga verksamhetsspecifika kontinuitetsplaner bör även samlas ihop på Kommunstyrelseförvaltningsnivå för central kvalitetssäkring och koordinering av regelbunden testning av kontinuitetsplanerna.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

6. Slutsats

Syftet med granskningen var att ge en övergripande nulägesanalys om huruvida Kommunstyrelsen för Haninge kommun har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

Efter utförd granskning har kommuncentral uppföljning av efterlevnad av informationssäkerhetsrutiner i Haninge kommuns koncernbolag och verksamheter identifierats som kommunens största förbättringsområde. Den generella mognadsnivån i kommunens arbete med informationssäkerhet bedöms annars vara god. I och med de befintliga styrdokumenten och de dedikerade informationssäkerhetsresurserna både i Kommunstyrelseförvaltningen och i verksamheterna finns det förutsättningar att bedriva ett ändamålsenligt arbete med informationssäkerhet på både kort och lång sikt.

Granskningens tre revisionsfrågor besvaras nedan:

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Hur ändamålsenlig är styrningen av arbetet med informationssäkerhet gentemot LIS-ramverket (i enlighet med MSB:s metodstöd och ISO27000) för de behov kommunens verksamhet har?	Styrningen av informationssäkerhetsarbetet i Haninge kommun gentemot LIS-ramverket bedöms vara delvis ändamålsenligt. Svaret grundar sig i att Haninge kommun har många fungerande komponenter på plats för att säkerställa ändamålsenlig informationssäkerhetsstyrning, bland annat styrdokument, dedikerade resurser och användaranvisningar, men brister finns rörande utbildningsinsatser och åtkomsthantering.	
Hur ändamålsenligt är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs?	Arbetet med uppföljning av efterlevnad av beslut och styrningsdokument relaterat till informationssäkerhet bedöms ej vara ändamålsenligt. Svaret grundar sig i att Haninge kommuns Kommunstyrelse inte tillsett att uppföljning av koncernbolagens, nämndernas och förvaltningarnas arbeten med informationssäkerhet genomförs, innefattandes exempelvis informationsklassning, objektsförvaltning, externa leverantörsavtal och kontroll av användares behörigheter.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Har Haninge kommun en ändamålsenlig incidenthanteringsprocess?	Haninge kommun bedöms ha en ändamålsenlig incidenthanteringsprocess. Svaret grundar sig i att Haninge kommuns incidentprocess är väl fungerande och utformad enligt god praxis med relevanta processteg, roller, forum och kompletterande användaranvisningar. Visst utrymme för förbättring finns i att definiera formella incidentrapporteringskrav till Kommunstyrelsen efter kritiska incidenter har åtgärdats.	

Stockholm, 5e mars 2019

Helena Törnqvist
EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

7. Bilaga 1: Definitioner

Förvaltningsledare: Verkställer objektsägares styrande anvisningar för ett förvaltningsobjekt och säkerställer att objektet i fråga förvaltas ändamålsenligt

Informationsklassning: Klassning av organisationens 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

Informationsägare: Äger och ansvarar för att informationen en verksamhet hanterar är riktig och tillförlitlig

IT-strateg: Förvaltningsspecifik roll som omsätter verksamheternas IT-relaterade behov till kravställningar mot Kommunstyrelseförvaltningen och agerar som länk mellan kommunen och verksamheterna i informationssäkerhetsarbetet

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

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

Objektsägare: Äger och har övergripande ansvar för ett förvaltningsobjekt och dess styrning och användning

Objektsspecialist: Stöder förvaltningsledaren i det operationella arbetet för ett förvaltningsobjekt och ser till att funktionalitet upprätthålls och aktiviteter utför

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

8. Bilaga 2: Källförteckning

Intervjuade roller:

- Chief Information Officer, chef för Digital Utveckling
- Lösningsarkitekt IT, Digital Utveckling
- Säkerhetsstrateg, Kommunstyrelseförvaltningen
- Kanslichef, Kommunstyrelseförvaltningen
- Dataskyddsombud

Dokumentation:

- Informationssäkerhetspolicy för Haninge kommun, 2016
- Informationssäkerhetsrelaterade anvisningar:
  - Anskaffning av IT-stöd
  - Privat användande av kommunens IT-arbetsplats
  - Hantering av känslig information i e-post
  - Molntjänster
  - Användarkonton
  - Användning IT- och telefonistöd
  - Guide lagring
- Incident Management Process, 2018
- Major Incident Procedure, 2018
- Lathund för Incidentrapportering, 2018
- Change Management Process, 2018
- Informationsklassning
- Förvaltningsmodell för förvaltning av Haninge kommuns IT-stöd, 2016
- Förvaltningsmodellen roller, 2017
- Roller i förvaltningsledningen
- IT – Haninge kommun, Organisation, uppdrag och styrning, revision 2.3
- Samverkanshandbok, 2017
- Utvecklingsprocessen