Deloitte.

JÖNKÖPINGS KOMMUN

Styrning av informationssäkerhet

Jönköpings Kommun

Juni 2019 – Torbjörn Bengtsson, Peter Birgersson, Louise Bredvik och Johan Eklöf

Innehåll

Sammanfattning

Deloitte AB har av de förtroendevalda revisorerna i Jönköpings kommun fått uppdraget att genomföra en granskning avseende informationssäkerhet.

Revisionsfråga

Bedriver kommunstyrelsen ett ändamålsenligt arbete med informationssäkerhet?

Svar på revisionsfråga

Vår sammanfattande bedömning är att kommunstyrelsen är i behov av förbättring för att uppnå ett ändamålsenligt arbete med informationssäkerhet.

Iakttagelser

- Roller och ansvar för informationssäkerhet, både på kommunnivå och inom förvaltningarna, är inte tydligt definierade.
- Formellt definierade rapporteringsvägar internt inom kommunen avseende informationssäkerhet saknas.
- Kommunen saknar en ändamålsenlig styrning av informationssäkerhet.
- Vi har noterat att kommunen saknar en formell process för uppföljning av informationssäkerhet.
- Informationssäkerhetspolicyn (”Program för informationssäkerhet”) är utdaterad. Policyn har sedan, tillägget 2011, inte uppdaterats årligen. Vidare saknas ett fullständigt ramverk för informationssäkerhet som beskriver hur verksamheten ska arbeta med informationssäkerhet.
- Metoden för informationsklassning och märkning av information inte är implementerat inom kommunen samt att man saknar en formell process för genomförande. Vidare saknas det även tillhörande styrdokument som beskriver roller och ansvar för genomförande, beskrivning kring processen för informationsklassningen samt märkning av information.
- En utbildningsplan samt genomförandet av utbildningsinsatser avseende informationssäkerhet saknas.
- Jönköpings kommun har till viss del en medveten organisation avseende informationssäkerhet, dock är medvetenheten baserad på erfarenhet snarare än via kontinuerlig utbildning.
- En övergripande riskanalys för informationssäkerhet inom kommunen har inte genomförts.
- En formaliserad process samt tillhörande styrdokumentation kring genomförandet av en riskanalys saknas.

Rekommendationer

Efter genomförd granskning rekommenderar vi kommunstyrelsen följande:

- Implementera en tydlig modell for styrning av informationssäkerhet och utse en informationssäkerhetschef med tillräckligt mandat för att implementera och följa upp informationssäkerhetsarbetet. Kommunen rekommenderas även att identifiera informationsägare inom organisationen som ska ansvara för implementera nödvändiga kontroller inom verksamheten.
- Etablera tydliga interna rapporteringsvägar för att säkerställa identifiering, hantering och uppföljning av informationssäkerhetsarbetet.
- Genomföra en övergripande riskanalys för att möjliggöra upprättandet av en plan och en strategi för informationssäkerhetsarbetet.

- Upprätta en process för hur de ska följa upp informationssäkerhetsarbetet, att man följer den strategi som definierats och att de implementerade kontrollerna mitigerar de noterade riskerna.

- Revidera existerande policy samt besluta och förankra de framtagna riktlinjerna för hur verksamheten ska arbeta operationellt med informationssäkerhet.

- Upprätta en tydlig och detaljerad instruktion över hur informationsklassificering och märkning av information ska genomföras. En process för genomförande av dessa bör även implementeras.

- Upprätta en allmän utbildning för anställda inom kommunen inom området informationssäkerhet. En utbildningsplan bör upprättas inkluderande utbildningsinsatser och aktiviteter som reflekterar de anställdas behov.

- Implementerar utbildningsinsatser avseende informationssäkerhet.

- Genomföra en övergripande riskanalys på kommunnivå för att fastställa strategiska mål för informationssäkerhet så att prioriteringen för investeringar genomförs där informationssäkerhetsbehoven är som störst.

- Etablera en formaliserad process för genomförandet av riskanalyser. Vidare bör man upprätta styrdokumentation kring genomförandet av riskanalyser.

Jönköping den 11 juni 2019

DELOITTE AB

Peter Birgersson
Senior Manager

Louise Bredvik
Senior Consultant

Torbjörn Bengtsson
Certifierad kommunal revisor

Johan Eklöf
Consultant

Inledning

Bakgrund

Informationssäkerhetshoten blir allt fler och tilltar i omfattning, vilket ökar kraven på kommuner att ha lämpliga processer, ansvarsfördelning samt rätt kunskap och kompetens inom verksamheten avseende informationssäkerhet. Förtroendevalda revisorerna har bedömt det som väsentligt att granska huruvida kommunens informationssäkerhetsarbete är ändamålsenligt. Revisorerna har därför gett Deloitte i uppdrag att genomföra granskning av kommunens arbete med informationssäkerhet.

Syfte och avgränsning

Granskningens syfte är undersöka om kommunstyrelsen bedriver ett ändamålsenligt arbete med informationssäkerhet. Granskningen begränsas till kommunstyrelsen och dess IT- och informationssäkerhetsverksamhet, med andra ord har inte styrning och kontroll över tredjeparter varit en del i denna granskning.

Revisionsfråga

Bedriver kommunstyrelsen ett ändamålsenligt arbete med informationssäkerhet?

Underliggande frågeställningar

- Främjar kommunstyrelsens IT organisation (med roller och ansvar) ett strategiskt informationssäkerhetsarbete?
- Finns ett välanpassat ramverk som beskriver hur verksamheten ska arbeta strategiskt/taktiskt/operationellt med informationssäkerhet för att uppnå önskad nivå på konfidentialitet, riktighet samt tillgänglighet?
- Genomförs utbildningsinsatser för att öka anställdas medvetenhet kring informationssäkerhet och främja en god säkerhetskultur på kommunen?
- Genomförs riskanalyser för att sätta strategiska mål för informationssäkerhet så att prioritering för investeringar genomförs där informationssäkerhetsbehoven är som störst?

Metod och granskningsinriktning

Granskningen har genomförts genom granskning av styrdokument, stickprovstestning för att verifiera faktisk efterlevnad inom ett antal utvalda områden samt genomförande av intervjuer med berörda inom kommunstyrelsens IT-organisation samt med IT-ansvariga för kommunens förvaltningar. Följande personer har intervjuats:

- Niklas Lingvall, IT-chef Jönköpings kommun

- Håkan Sonesson, tillförordnad IT-säkerhetsansvarig- och informationssäkerhetssamordnare
- Maria Ossiansson, Utvecklingschef Tekniska Kontoret (TK)
- Claes Axelsson, IT-strateg Utbildningsförvaltningen (UBF)
- Magnus Danielsson, IT-chef Socialförvaltningen (SF)

Granskningen har delats in i följande sju faser:

- Planering av intervjuer.
- Samla fakta/underlag genom intervjuer och dokumentgranskning.
- Genomgång, sammanställning och analys av insamlat material. Vid behov komplettering med mer material.
- Framtagning av viktiga iakttagelser och rekommendationer samt svar på revisionsfråga.
- Rapportskrivning inkl. sakavstämning.
- Presentation av granskning till revisorer.
- Godkänd rapport skickas till berörda nämnder & revisorer.

Kvalitetssäkring

Kvalitetssäkring har skett genom Deloittes interna kvalitetssäkringssystem. Rapporten har även kvalitetssäkrats av de intervjuade personerna.

Granskningsresultat

Utifrån genomförda intervjuer och granskat material har en övergripande beskrivning av kommunens informationssäkerhetsarbete gjorts nedan. De iakttagelser som framkommit till följd av intervjuer och dokumentstudier redogörs under den rubrik som ansetts mest lämplig.

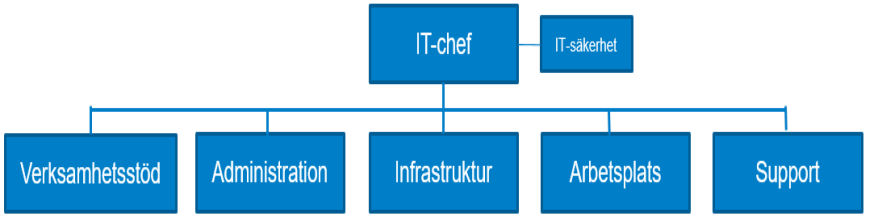
Främjar kommunstyrelsens IT organisation (med roller och ansvar) ett strategiskt informationssäkerhetsarbete?

Roller och ansvar

Informationssäkerhetsansvaret är i dagsläget en del av den IT-säkerhetsansvarigas arbetsuppgifter som är placerad inom Jönköping kommuns IT-avdelning. IT-avdelningens organisation består av en IT-chef som är ytterst ansvarig och där den IT-säkerhetsansvarig är direkt underställd IT-chefen. IT-avdelningen är en stödfunktion inom kommunen vilket innebär att de har ansvaret för att supportera och tillse förvaltningarna med IT, vilket innefattar exempelvis infrastruktur och support. IT-avdelningen ska äga frågan om samordningen av informationssäkerhet, men IT-avdelningen saknar mandat för att driva arbetet vidare som stödfunktion till kommunen.

Informationssäkerhetssamordnaren saknar en tydlig definition vad samordningen innefattar och vad rollen som informationssäkerhetssamordnare innebär. Det saknas även en tydlig roll- och ansvarsfördelning avseende informationssäkerhetsarbetet inom kommunen och dess förvaltningar.

IT-avdelningens organisation



Under granskningen blev vi informerade om att det pågår en dialog och det finns ett önskemål hos IT-avdelningen inom kommunen att anställa en informationssäkerhetssamordnare på heltid.

Rapporteringsvägar

IT-säkerhetsansvarig rapporterar direkt till IT-chefen i nuvarande organisationsstruktur. IT-säkerhetsansvarig har inga formella krav på rapportering avseende informationssäkerhetsarbetet, och i dagsläget görs det i ostrukturerat format baserat på aktuella utmaningar, problem eller frågeställningar. Det saknas även formella krav för hur förvaltningarna rapporterar vidare informationssäkerhetsrelaterade utmaningar, problem och frågeställningar. IT-chefens rapportering kring informationssäkerhet till stadsdirektören och kommunstyrelsen saknar även formella krav och struktur.

Inom IT-avdelningen har IT-chefen samt IT-säkerhetsansvarig ett informellt ansvar att internt rapportera informationssäkerhets- och personuppgiftsincidenter, dock saknas en tydlig struktur eller krav på vilka roller som innehar det formella ansvaret för den interna rapporteringen.

Bedömning

Vi noterade att det inte förekommer tydligt definierade roller och ansvar för informationssäkerhet, både på kommunnivå och inom förvaltningarna. Mandat saknas även för den utsedda informationssäkerhetssamordnaren för att implementera och genomföra uppföljning av informationssäkerhetsarbetet inom kommunen.

Under granskningen noterades det även att man saknar formellt definierade rapporteringsvägar internt inom kommunen för hantering av informationssäkerhetsrisker, informationssäkerhetsincidenter och uppföljning av informationssäkerhetsarbetet.

Rekommendation

Vi rekommenderar kommunstyrelsen att implementera en tydlig modell for styrning av informationssäkerhet. Kommunen bör se över och definiera vilka roller och ansvar som bör finnas inom organisationen, på både kommunnivå och inom förvaltningarna för att kunna främja ett strategiskt informationssäkerhetsarbete. Vidare rekommenderas kommunstyrelsen att utse en informationssäkerhetschef med tillräckligt mandat för att implementera och följa upp informationssäkerhetsarbetet.

Den utsedda informationssäkerhetschefen bör inte ha en konflikterande roll, exempelvis genom att utse IT-säkerhetsansvarig till informationssäkerhetsansvarig. Informationssäkerhetschefen är ansvarig för att sätta ramverk och kontroller samt följa upp dessa, medan den IT-säkerhetsansvarig ansvarar för att implementera dessa. Kommunen rekommenderas även att identifiera informationsägare inom organisationen som ska ansvara för att implementera nödvändiga kontroller inom verksamheten.

Vi rekommenderar att kommunstyrelsen etablerar tydliga interna rapporteringsvägar för att säkerställa identifiering, hantering och uppföljning av informationssäkerhetsarbetet.

Finns ett välanpassat ramverk som beskriver hur verksamheten ska arbeta strategiskt/taktiskt/operationellt med informationssäkerhet för att uppnå nivå på konfidentialitet, riktighet samt tillgänglighet?

Styrning av informationssäkerhet

Avseende styrning av informationssäkerhet så har man inte tagit fram en formell plan eller definierat en strategi för informationssäkerhetsarbetet. I dagsläget finns det tre framtagna principer som den tillförordnade (t.f.) IT-säkerhetsansvarige tillsammans med IT-chefen tagit fram för att prioritera och sätta en riktning på informationssäkerhetsarbetet. Dessa tre principer är:

- Informationssklassning
- Riskanalys
- Utbildning

Enligt informationssäkerhetspolicyn för informationssäkerhet ska policyn samt tillhörande riktlinjer och instruktioner, löpande följas upp och vid behov revideras. Under granskningen noterades att det inte sker ingen strukturerad uppföljning av informationssäkerhetsarbetet och inte heller av kraven i policyn.

Ramverk för informationssäkerhet (policy, riktlinjer och rutiner)

Det finns en informationssäkerhetspolicy (”program för informationssäkerhet”) som upprättades 2008 och som revideras 2011. Det är den senast antagna och godkända policyn. Den policy som finns från 2008 gäller fortfarande och innehåller mål och omfattning samt generella krav som ska efterföljas. Under granskningen noterades att man i inte alltid efterlever policyn.

Jönköping kommun har supporterats av ett externt konsultföretag som under 2018 tog fram generella riktlinjer för informationssäkerhet. Riktlinjerna bygger på ISO27001/2 och har tagits fram baserat på god praxis. Riktlinjerna innehåller informationssäkerhetskrav för medarbetare, styrning av informationssäkerhet, informationssäkerhet i verksamheten samt informationssäkerhet i IT-miljön. Riktlinjerna har inte antagits och därmed inte förankrats inom organisationen.

Informationsklassning

Baserat på de definierade principerna för informationssäkerhet har man tagit fram en metod för informationsklassificering och en kategorisering för att märka information. Klassificeringsmodellen omfattar tre informationssäkerhetsaspekter, som även omnämns i informationssäkerhetspolicyn; konfidentialitet, riktighet och tillgänglighet. Kategorier för bedömning av konsekvenser görs enligt; Synnerligen, Allvarlig, Betydande och Måttlig. Kategorisering för att märka information görs enligt; Öppen, Intern och Hemlig.

Ett systemstöd för genomförande av informationsklassning har även implementerats för stärka arbetet med klassning. Det nya systemstödet kommer att presenteras för IT-ledningen under Q3 2019.

För att påbörja implementationsarbetet av informationsklassningen har man i dagsläget identifierat 10 informationssäkerhetsobjekt som anses vara mer kritiska för kommunen som inledningsvis kommer att klassificeras. Detta arbete informerades vi om är påbörjat. Men man saknar en formaliserad process för genomförandet av informationsklassning och märkningen av information samt att informationsklassning och märkningen av information

inte är implementerad i verksamheten.

Bedömning

Vi noterade att kommunen saknar en ändamålsenlig styrning av informationssäkerhet.

Vidare noterade vi att kommunen saknar en formell process för uppföljning av informationssäkerhet.

Vi noterade att den upprättade informationssäkerhetspolicyn (”Program för informationssäkerhet”) är utdaterad. Policyn har sedan, tillägget 2011, inte uppdaterats årligen. Vidare saknas ett fullständigt ramverk för informationssäkerhet som beskriver hur verksamheten ska arbeta med informationssäkerhet.

Under granskningen noterade vi även att metoden för informationsklassning och märkning av information inte är implementerat inom kommunen samt att man saknar en formell process för genomförande. Vidare saknas det även tillhörande styrdokument som beskriver roller och ansvar för genomförande, beskrivning kring processen för informationsklassningen samt märkning av information.

Rekommendation

Vi rekommenderar kommunstyrelsen att genomföra en övergripande riskanalys för att möjliggöra identifiering av mål med informationssäkerhetsarbetet. Vidare rekommenderar vi att de definierade målen för informationssäkerhet ska utgöra grunden till upprättandet av en plan och en strategi för informationssäkerhetsarbetet.

Fortsättningsvis rekommenderas kommunstyrelsen att man upprättar en process för hur de ska följa upp informationssäkerhetsarbetet, att man följer den strategi som definierats och att de implementerade kontrollerna mitigerar de noterade riskerna.

Vi rekommenderar att kommunstyrelsen reviderar existerande policy samt besluta och förankra de framtagna riktlinjerna för hur verksamheten ska arbeta operationellt med informationssäkerhet. Om nödvändigt, bör kommunen även ta fram detaljerade rutiner och instruktioner för att vidare detaljera hur de riktlinjerna ska efterlevas.

Vi rekommenderar kommunstyrelsen att upprätta en tydlig och detaljerad instruktion över hur informationsklassificering och märkning av information ska genomföras. Vidare rekommenderar vi att man implementera en process för genomförande av dessa i organisationen. Instruktionen bör även inkludera roller och ansvar för genomförande och uppföljning, både på kommunnivå samt inom förvaltningarna.

Genomförs utbildningsinsatser för att öka anställdas medvetenhet kring informationssäkerhet och främja en god säkerhetskultur på kommunen?

Utbildning och medvetenhetsgörande aktiviteter

Den nuvarande utbildningen som finns tillgänglig för anställda finns på intranätet är en utbildning framtagen av Myndigheten för Samhällsskydd och beredskap (MSB). Under granskningen blev vi även informerade om att kommunen planerar att köpa in verktyg för att genomföra mindre utbildningar, så kallade nano-Learnings, för anställda.

Utbildning för anställda och nyanställda sker emellanåt på förvaltningsnivå och det finns ingen gemensam utbildning på kommunnivå. Inom förvaltningarna så brister utbildningen för befintligt anställda samt nyanställda avseende informationssäkerhet då det inte sker på ett strukturerat eller enhetligt sätt inom kommunen.

Senaste året har informationssäkerhet, i och med implementationen av GDPR, varit ett aktuellt ämne. Exempelvis har man inom UBF haft en stor utbildningsinsats inom personuppgiftshantering och vid nyanställning på TK är det enbart Dataskyddsförordningen som man utbildar den nyanställda inom.

Bedömning

Vi har under granskningen noterat att det inte genomförs utbildningsinsatser kring informationssäkerhet. Det saknas en utbildningsplan för att säkerställa kontinuerlig utbildning och aktiviteter för att öka medvetenheten kring informationssäkerhet. Vidare saknas en process för att följa upp att genomförda utbildningar har haft avsedd effekt.

Jönköpings kommun har till viss del en medveten organisation avseende informationssäkerhet, dock är medvetenheten baserad på erfarenhet snarare än via kontinuerlig utbildning.

Rekommendation

Vi rekommenderar att kommunstyrelsen tar fram en allmän utbildning för anställda inom kommunen inom området informationssäkerhet. Vi rekommenderar att en utbildningsplan upprättas inkluderande utbildningsinsatser och aktiviteter som reflekterar de anställdas behov. Planen bör omfattas av en uppföljningsprocess för att utvärdera att genomförd utbildning haft avsedd effekt och om utbildningsplanen behöver revideras.

Utbildningsinsatser bör implementeras i det befintliga utbildningsmaterialet som existerar inom vissa förvaltningar, exempelvis den introduktionsutbildning som ges inom Socialförvaltningen. I förvaltningar där det inte existerar någon utbildning bör det implementeras från grunden samt på ett enhetligt sätt.

Genomförs riskanalyser för sätta strategiska mål för informationssäkerhet så att prioritering för investeringar genomförs där informationssäkerhetsbehoven är som störst?

Riskanalys för informationssäkerhet

Enligt policyn som finns upprättad ska det utföras riskanalyser på samtliga informationssystem. Under granskningen kunde man inte verifiera att riskanalyser skett på samtliga informationssystem. Tidigare har det utförts risk- och sårbarhetsanalyser (RSA) inom kommunen, men metoden var omfattande och har inte använts kontinuerligt inom verksamheten.

Baserat på de definierade principerna för informationssäkerhet har man tagit fram en ny metod för riskanalyser. Metoden är inte formaliserad och det saknas en process för genomförande. Metoden för riskanalyser är ännu inte etablerad inom organisationen.

Inom TK har de avdelningar med kritisk infrastruktur (exempelvis Vatten & Avlopp (VA)) strikt säkerhetshantering. Det innebär bland annat att man genomför generella riskanalyser kontinuerligt som en del i sitt säkerhetsarbete. Riskanalyserna avser inte specifikt informationssäkerhet, men det finns en process kring genomförandet av dem.

Bedömning

Vi har noterat att det inte har genomförts en övergripande riskanalys för informationssäkerhet inom kommunen. Avsaknaden av en övergripande riskanalys medför att man inte har upprättat strategiska mål för informationssäkerhetsarbetet samt att man saknar en fullständig uppfattning kring behovet av informationssäkerhetskontroller. Vidare har man inte kunnat dra slutsatser kring vilka områden som bör prioriteras avseende information- och IT-säkerhet och där behovet av säkerhet är som störst.

Fortsättningsvis saknas en formaliserad process samt tillhörande styrdokumentation kring genomförandet av en riskanalys.

Rekommendation

Vi rekommenderar att genomföra en övergripande riskanalys på kommunnivå för att fastställa strategiska mål för informationssäkerhet så att prioriteringen för investeringar genomförs där informationssäkerhetsbehoven är som störst.

Vidare rekommenderas kommunstyrelsen att man etablerar en formaliserad process för genomförandet av riskanalyser. Vi rekommenderar även att man upprättar styrdokumentation kring genomförandet av riskanalyser, roller och ansvar för genomförande och implementation av åtgärder samt hur resultatet av genomförd riskanalys ska ligga till grund för kommunens strategiska, taktiska och operationella mål och arbete med informationssäkerhet.

För TK bör man se över om det går att implementera riskanalyser avseende informationssäkerhet i den befintliga processen för riskanalyser.

Deloitte.