Nacka kommun

Revisorerna

Revisionsskrivelse

2017-09-25

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Granskning av IT- och informationssäkerhet

Vår revisionsplan för 2017 omfattar bl a revision av hur Nacka kommun arbetar med IT-säkerhet och informationssäkerhet. EY har på uppdrag av oss revisorer granskat hur Nacka kommun arbetar med IT- och informationssäkerhet (Revisionsrapport nr 3/2017).

Granskningen omfattar en stor mängd revisionsfrågor. Dessa har besvarats genom en granskning mot så kallad god praxis inom informationssäkerhetsområdet. Granskningen har gjorts mot utvalda delar av EY:s ramverk Cyber Program Assessment. Ramverket bygger på de svenska och internationella standarderna ISO/IEC 27000, COBiT och ITIL. EY har genomfört en övergripande kartläggning av rutiner, kontroller samt IT-säkerheten. Det ramverk som använts för granskningen har inga preferenser i sig om outsourcing av IT-verksamhet är bättre eller sämre ur intern kontrollsynpunkt. Huruvida IT-verksamheten är outsourcad eller inte kräver dock olika överväganden vad gäller utformning av den interna kontrollen.

Nacka kommun har interna resurser som är ansvariga och engagerade i frågorna och arbetar med att ta fram processor och ramverk som kan stödja den nya dataskydds-lagstiftningen. Granskningen visar att Nacka kommun i stort har goda förutsättningar för ett ändamålsenligt arbete med informationssäkerhet. Dock saknas processer och rutiner i nuläget för att effektivt kunna arbeta med dessa frågor och för att säkerställa en tillräcklig intern kontroll inom området. Kommunens starka sidor finns inom områdena tredjepartsleverantör, personalresurser och förberedelse för implementation av GDPR. Förbättringsområden har identifierats främst inom information och utbildning, efterlevnad av styrdokument, rutiner för behörighetsadministration och hantering av telefonmeddelanden och sms.

Utifrån den granskning som har gjorts vill vi särskilt lyfta fram följande:

- Av granskningen ser vi revisorer att kommunens decentraliserade organisation ur ett internkontrollperspektiv ställer stora krav på att tydliggöra ansvaret för IT- och informationssäkerheten. Vi ser inte att kommunen tillräckligt uppmärksammat detta. Var finns till exempel den centralt placerade personen som är ytterst ansvarig för dessa frågor?
- Kommunen saknar standardiserade och definierade rutiner och processer kring informationssäkerhet samt styrning av dessa. Detta innebär risk att organisationens olika ansatser inom informationssäkerhet inte genomförs på ett enhetligt och målinriktat sätt och utan en övergripande struktur. Det rekommenderas att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig informationssäkerhetsbild. Efter att granskningen påbörjades och intervjuer genomförts har ett styrdokument tagits fram, benämnt "Samverkansmodell Nacka."
- Kommunen har inte uppdaterat sin informationssäkerhetspolicy på tre år, vilket innebär en risk för att den inte är anpassad efter förändrade omständigheter i

organisationen och omvärlden. Vi rekommenderar att policyn ses över löpande, åtminstone en gång per år.

- Kommunen genomför inga utbildningsinsatser inom området informationssäkerhet. I och med detta riskerar bristande kunskap och medvetenhet exponera och utsätta organisationen för informationssäkerhetsrisker. Det rekommenderas att ett strukturerat utbildningsinitiativ startas. Enligt uppgift planeras för en utbildningsinsats av samtliga medarbetare under hösten 2017.
- Kommunen saknar tillräckliga incidenthanteringsrutiner och processer kring informationssäkerhet, samt en gedigen incidentshanteringsplan. Detta medför risk för att eventuella brister eller incidenter inte åtgärdas. Vi rekommenderar att riktlinjer, rutiner och processer etableras och sprids i organisationen. Efter att granskningen påbörjades och intervjuer genomförts har ett styrdokument tagits fram, benämnt "Samverkansmodell Nacka."
- Kommunen har i nuläget roller med ansvar inom informationssäkerhet, dock är dessa spridda i organisationen. Det saknas en dedikerad avdelning eller grupp som äger dessa frågar och driver de fullt ut – med t.ex. kompletta rutinbeskrivningar samt etablering av behörighetsadministrationsprocesser.
- Kommunen genomför inte några penetrationstester utan förlitar sig helt på tredjepartsleverantörer och verksamhetsenheter inom den decentraliserade organisationen. Penetrationstester syftar till att identifiera tekniska sårbarheter som kan vara blottade för en eventuell angripare. Kommunen genomför i dagsläget inga externa penetrationstester, dvs. tester utifrån ett externt angreppsutfall, och inga interna penetrationstester, dvs. tester utifrån ett insiderperspektiv

Vi önskar svar från kommunstyrelsen på noterade brister och förbättringsområden enligt bifogad rapport senast den 30 november 2017. Vi avser att bjuda in kommunstyrelsen för att diskutera svaret.

För revisorerna i Nacka kommun

Lars Berglund
Ordförande

Yvonne Wessman
Vice ordförande

Bilaga: Revisionsrapport nr 3/2017 – IT- och informationssäkerhet