Deloitte.

Uppföljande granskning 2017

Kommunstyrelsen
Socialnämnden

Revisionsrapport 2017-09-15

Sammanfattning

I rapporten sammanfattas resultat av uppföljande granskning av IT säkerhet 2014, 2016. Granskningen 2014 syftade till att undersöka om den interna kontrollen avseende IT säkerhetsarbetet fungerar tillfredsställande. Uppföljningens syfte 2016 och denna är att följa upp och bedöma om nämndernas internkontrollarbete är tillräckligt. Utgångspunkter är de rekommendationer som lämnats i ursprunglig fördjupningsgranskning. De väsentligaste iakttagelserna är följande:

Arbeten för att säkra system enligt ISO/IEC 27000:1 pågår. IT ansvarig vid kommunledningsförvaltning arbetar tillsammans med verksamhetsansvariga och systemförvaltare vid förvaltningarna. Ansvarsroller framgår av systemen eller via manuella förteckningar. Rutiner för regelbundna kontroller av säkerheter i system, att system uppdateras och ajourhålls, kommer att tas fram inom utvecklingsarbetet enligt ISO standarden. Utgångspunkter för informationssäkerhetsarbetet finns i IT säkerhetspolicyn sedan 2004. Någon övergripande analys och/eller samlad bild av kommunens informationssäkerhetsnivå finns inte i dagsläget. Uttryckta behov i ursprunglig granskning om ett mer strukturerat arbete när det gäller informationssäkerheten kvarstår. Kommunen behöver säkerställa att ett systematiskt säkerhetsarbete bedrivs på alla nivåer.

Uppföljningen har begränsats till ett fåtal frågeställningar och ger inte underlag för en bedömning om nämndernas internkontrollarbete är tillräckligt.

Rekommendationer

Kommunstyrelsen bör överväga att med utgångspunkter i MSB:s (Myndigheten för samhällsskydd och beredskap) föreskrifter och allmänna råd, MSBFS 2016:1, ta fram en analys av nuläget och skapa en handlingsplan utifrån nuläget. Därefter revideras riktlinjer och styrdokument som gör det möjligt för organisationen att efterleva ställda krav. Återkommande uppföljningar vars resultat ingår som en del av återrapporteringen i nämnden behövs.

IT säkerhet 2014, 2016

Granskning	Resultat
Organisering Rutiner Anvisningar	NY IT organisation beslutades av kommundirektören i september 2016. I IT enhetens uppgifter ingår att utforma anvisningar och rutiner utifrån centralt beslutade strategier och policys. Det innefattar att initiera säkerhetshöjande aktiviteter och att arbeta med hot-, risk- och sårbarhetsanalyser inom IT området. En IT handläggare har anställts vid kommunledningsförvaltningen som arbetar med IT säkerhet. Arbeten med tillgänglighetsanalys och informationsklassning av system pågår enligt ISO/IEC 27000:1. Rutiner för regelbundna kontroller kommer att tas fram inom detta arbete. Arbetet med tillgänglighetsanalyser och informationsklassning görs tillsammans med verksamhetsansvarig och systemförvaltare. Förvaltningschef är systemägare (socialförvaltningen). Ansvaret att uppdatera ansvarsroller är systemägarens och som utförs manuellt via inventariesystem eller manuell lista en gång per år.
Risk- och konsekvensanalys	Risk- och konsekvensanalyser ska göras i samband med upphandling av IT system. När det gäller förändringar/kompletteringar kring befintliga system finns risk- och konsekvensanalysen med i en årlig systemförvaltningsplan.
Exempel på kontrollmoment	Av internkontrollplaner framgår att behörigheter gås igenom minst en gång per år och samkörs med lönesystemet. Rutin för sekretess i verksamhetssystem (socialförvaltningen) hanteras enligt särskild rutin. Information lämnas vid introduktion av nyanställda när anställningen påbörjas och vid informationsdagar.

IT säkerhet 2014, 2016

Granskning	Resultat
Forum/ansvar	IT enheten har utsett kundansvariga för varje förvaltning som arbetar med att stödja förvaltningen i IT frågor. Kundansvariga träffas regelbundet för utbyta av informationer om vad som sker vid förvaltningarna. För de kommungemensamma systemen finns systemförvaltarna inom IT enheten. Ansvaret för att uppdatera och ajourhålla system är systemägarens. För att se att det fungerar lämnades uppgiften i svar på ursprunglig granskning att en årlig granskning skulle genomföras. Uppföljning kommer att göras inom ram för pågående utvecklingsarbete enligt ISO standard.
Informationer i nämnd	Övergripande informationer om IT säkerhet lämnas i kommunstyrelsen. Informationer och beslut kring mera detaljerade IT säkerhetsåtgärder tas upp i den nyligen bildade strategiska IT beredningsgruppen. Gruppen har att samordna och prioritera aktiviteter i IT-planen och att verka för att IT bidrar till att kommunövergripande mål nås. Handläggare för IT säkerhet vid kommunledningsförvaltningen har periodiska avstämningar med kommunens säkerhetschef. Kontroller kopplat till IT säkerhet följs upp i den årliga internkontrollplanen i nämnd.