SEKRETESS OSL (2004:400) 18 KAP § 13

Danderyds kommun

Granskning av informationssäkerhet

Oktober 2022

Kristian Damlin (Kristian.damlin@pwc.com) - Uppdragsledare
Nur Nauti (Nur.nauti@pwc.com) - Projektledare
Carl Nisser (Carl.nisser@pwc.com) - Projektmedlem

pwc

Innehållsförteckning

1. Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Danderyds kommun genomfört en granskning av informationssäkerhet. Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Vår sammanfattande revisionella bedömning grundar sig i de bedömningar som görs av de revisionsfrågor som ingår i granskningen. Efter genomförd granskning är den samlade bedömning att Danderyds kommuns kommunstyrelse **inte helt** säkerställer ett ändamålsenligt informationssäkerhetsarbete och att detta sker med tillräcklig intern kontroll. Detta då kommunstyrelsen idag inte genomför någon systematiskt kravställning och uppföljning att kommunens verksamheter fullgör sina uppgifter inom informationssäkerhetsområdet. Enligt erhållna intervjusvar sker viss muntlig rapportering om kommunens informationssäkerhetsarbete av informationssäkerhetssamordnare till kommunstyrelsen, arbetet är däremot inte dokumenterat.

Då kommunstyrelsen är informationsägare och därmed även riskägare är det kommunstyrelsen som måste delegera och säkerställa att riskanalyser genomförs systematiskt och att risker åtgärdas. Idag finns det inte en tillräcklig kontroll och uppföljning av att risker identifieras, varken för kommungemensamma eller verksamhetsspecifika system.

PwC har noterat att IT-avdelningen inom Danderyds kommun har flera pågående, positiva arbetsinsatser för att förbättra arbetet med IT- och informationssäkerhet. Exempelvis finns ett pågående arbete i att upphandla IT-säkerhetssamordnare som tjänst med målbild att stärka kommunens säkerhetsarbete på operativ, taktisk samt strategisk nivå. IT-avdelningen har, trots sin begränsade storlek, ett stort ansvar över många av verksamhetens frågor, ställningstaganden och uppgifter för kommunens leveransförmåga kopplat till den digitala infrastrukturen.

För att optimera informationssäkerhetsarbetet inom kommun rekommenderar vi att verksamheten ansvarar för prioriteringar av informationssäkerhetsfrågor. Ansvarsfördelning som beställare och utförare mellan verksamhet och IT-avdelning behöver förtydligas för att skapa effektivitet i processer kopplat till IT- och informationssäkerhet och hanteras fördelaktigt genom att införliva, förtydliga och förankra befintlig systemförvaltningsmodell samt inkludera informationssäkerhetsrelaterade aktiviteter till roller som systemägare, systemförvaltare etc.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet “*Sammanfattande bedömningar utifrån revisionsfrågor*”.

Revisionsfrågor	**Bedömning**
Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	**Delvis** 
Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?	**Delvis** 
Finns ett ledningssystem för informationssäkerhet implementerat?	**Delvis** 
Sker kommunens arbete med informationssäkerhet systematiskt?	**Delvis** 

1. Sammanfattning forts.

PwCs har noterat ett antal områden där informationssäkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll av informationssäkerhet och ett förbättrat informationsägarskap för kommunstyrelsen. Följande är ett urval av rekommendationer.

PwC rekommenderar kommunstyrelsen att;

- Intensifiera arbetet med att utveckla systemförvaltningsmodellen i syfte att förankra informationssäkerhetsrelaterade ansvarsområden i verksamheterna.
- Säkerställa att verksamheterna organiserar sig unisont inom deras arbete med informationssäkerhet för att få genomslag och synergier av varandras informationssäkerhetsarbete.
- Säkerställa att ansvariga inom området har tillräckligt med resurser och mandat för att bedriva ett ändamålsenligt informationssäkerhetsarbete enligt framtagna riktlinjer och förvaltningsmodell.
- Öka medvetenheten gällande de styrande dokumenten och sprida kunskaper om deras innehåll med fokus på implementering och efterlevnad.
- Ta fram genomförandeplan för hur efterlevnad av riktlinjer för medarbetare ska säkerställas.
- Formalisera och utvärdera möjlighet att inkludera regelbundet återkommande arbetsmoment och kontroller mht IT- och informationssäkerhet i som en del av övriga internkontrollplaner samt systemförvaltningsplaner.
- Intensifiera genomförande av mer omfattande riskanalys på systemnivå med bäring på IT- och informationssäkerhet. Det är förvaltningarna som ska ha ansvaret för att driva identifieringen av risker och de informationstillgångar som är relevanta att skydda, men att centrala funktioner tillhandahåller nödvändig resurser, mandat och tydliga roller för att stödja dess genomförande.
- Fastställa vad som för kommunen är verksamhetskritiska system samt att påbörja klassificering av detsamma. Vidare rekommenderas kommunen att framställa och dokumentera metod för klassificering i styrande dokumentation. Det är av vikt att ha kännedom om vilka system som är kritiska för verksamheten för att bland annat kunna kravställa vad outsourcingsleverantörer ska prestera samt för att fastställa ändamålsenliga informationssäkerhetskrav i befintliga och kommande avtal.
- Utveckla övergripande kontinuitetsplan för att säkerställa att verksamheten har effektiva processer, system och stöd för att motverka långvariga avbrott i verksamheten. Kontinuitetsplan kan ses som kravställare till IT-avdelningen och andra samarbetspartners vid utformning av avbrottsplan.
- Utveckla avbrottsplaner, innefattande hur allvarliga avbrottssituationer ska hanteras och nödvändiga åtgärder för att få tillbaka IT-stödet enligt verksamhetens krav, samt testa planen regelbundet.
- Ställa tydliga krav gentemot leverantören på förväntad leverans inom olika områden gällande exempelvis drift, avbrottsplanering och infrastruktur. Uppfyllande av dessa krav som finns ska även från leverantörens sida kunna påvisas, exempelvis i rapportform. Kommunstyrelsen rekommenderas även att utvärdera ifall det finns ett behov av att ta in en tredje part för att verifiera och säkerställa att informationssäkerhetskrav som ställs i avtalen är ändamålsenliga.
- Ta fram rutin att inkludera kommunledningen årligen i hur det fortlöpande arbetet med informationssäkerhet går.
- Införa tydlighet kring obligatoriska, regelbundna utbildningsmoment för samtliga medarbetare. Utbildningarna bör utgå från ett informationssäkerhetsperspektiv och inte vara sprunget ur ett GDPR-hänseende.
- Genomför incidentövningar för prioriterade hot som beskriver roller, ansvar och aktiviteter i syfte att öka förmågan att effektivt reagera och hantera en storskalig IT-incident.

2

Inledning

- Bakgrund
- Syfte och revisionsfrågor
- Revisionskriterier
- Avgränsning
- Metod

2. Inledning

Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag eftersom en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild säkerhetsincident. Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Klassning av informationstillgångar är viktigt för att säkerställa att den mest skyddsvärda informationen verkligen får det skydd som krävs.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet och konfidentialitet.

Information är värdefull och behöver många gånger skyddas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering, vilket skapar förtroende både inom och utanför organisationen.

Utmaningar gällande informationssäkerhet har även resulterat i NIS-direktivet, som i korthet innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga- och vissa digitala tjänster, både för privata och offentliga aktörer. Förslaget till direktiv, NIS 2, inkluderar bl.a. hårdare säkerhetskrav samt ett sanktionssystem.

Revisorerna har i sin riskanalys för 2022 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att finns en god informationssäkerhet inom kommunen och har därför gett PwC ett uppdrag att granska området.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Följande revisionsfrågor har bedömts som viktiga för granskningen:

1. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
2. Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?
3. Finns ett ledningssystem för informationssäkerhet implementerat?
4. Sker kommunens arbete med informationssäkerhet systematiskt?

Revisionskriterier

- Kommunallagen
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2017)

2. Inledning

Avgränsning

I tid avgränsas granskningen till år 2022 samt till granskningens kontrollfrågor. Vidare har eventuella resultat från denna granskning inte validerats för att bedöma utförandet av kontrollerna i omfattningen. Bedömningen har baserats på den inkomna dokumentationen och de intervjuer som genomförts med identifierade intressenter.

Metod

Granskningen har genomförts med hjälp av intervjuer av identifierade nyckelpersoner i kommunen, samt inläsning och genomgång av tillgänglig dokumentation. För lista över dokumentationen se sidan 17.

De funktioner som intervjuats inom ramen för granskningen är följande:

- Informationssäkerhetssamordnare
- Säkerhetsskyddschef
- IT-chef
- Socialförvaltningens stabschef

Granskningen har genomförts mellan augusti och oktober 2022 av Nur Nauti och Carl Nisser (PwC) och kvalitetssäkrats av Kristian Damlin (uppdragsledare) på PwC samt faktakontrollerats av företrädare i Danderyds Kommun.

Granskningsresultat

- **Revisionsfråga 1**: Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
- **Revisionsfråga 2**: Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?
- **Revisionsfråga 3**: Finns ett ledningssystem för informatinssäkerhet implementerat?
- **Revisionsfråga 4**: Sker kommunens arbete med informationssäkerhet systematiskt?

3. Resultat av granskning

3.1 Revisionsfråga 1: *Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?*

Iaktagelser

Danderyds kommun har en informationssäkerhetspolicy som är från år 2019 för vilket kommunens informationssäkerhetsarbete utgår från. Policyn är beslutad av kommunfullmäktige och i policyn fastslås det att ansvar för det kontinuerliga informationssäkerhetsarbetet följer linjeansvar vilket innebär att varje nämnd är ansvarig för att tillräckliga åtgärder vidtas för den informationen som nämnden ansvarar för att hantera. Arbetet ska vara långsiktigt, löpande och omfatta hela verksamheten samt samtliga informationstillgångar.

Under policyn har kommunen tagit fram en anvisning "*Anvisning organisation för säkerhet och dataskydd*" som än mer tydliggör olika roller och ansvarsområden inom arbetet för informationssäkerhet. I denna anvisning samt utifrån intervjuer framgår att det centralt i kommunen finns en informationssäkerhetsorganisation bestående av informationssäkerhetssamordnare och säkerhetschef vars uppgift är att ta fram styrande dokument samt agera stöd åt organisationen. Anvisningen beskriver även detaljerat vilket ansvar olika delar av organisationen har, exempelvis vad en nämnd eller förvaltningschef ansvarar för. Detta inkluderar att vara förenliga med gällande lagstiftning, policys och riktlinjer samt säkerställa att underlydande enhetschefer vidtar tillräckliga åtgärder för att upprätthålla säkerhet inom deras respektive enheter.

Det primära kontinuerliga informationssäkerhetsansvaret ute förvaltningarna faller inom kommunens framtagna systemförvaltarmodell. I systemförvaltningsmodellen framgår att det är systemägare som i egenskap av informationsägare skall inkludera informationssäkerhet i sina förvaltningsplaner. En nyckelroll kommunen har definierat är vad som kallas *kontaktombud.* Kontaktombuden utses av förvaltningarna och skall agera stödjande i förvaltningens arbete med informationssäkerhet och dataskydd (GDPR) och delta i förvaltningsöverskridande nätverk för att dela erfarenheter och kunskap.

Kommunens strukturering av roll- och ansvarsfördelning av informationssäkerhet är väl definierat. Dock framgår det under intervjuer att förankring är bristande. Detta tydliggörs under intervjuer då verksamheterna inte har en unison syn av innebörden av systemförvaltningsmodell vilket i kombination med resursbrist resulterar i att nyckelaktivieter kopplat till informationssäkerhet inte genomförs.

Granskningen visar även att kontaktombudens arbete med informationssäkerhet i praktiken tenderar att primärt fokusera på rutiner och processer kring personuppgiftshantering snarare än att efterleva framtagna ledningssystem för informationssäkerhet (LIS), vilket omfattar ett större antal aktiviteter än enbart de som är drivna ur ett dataskyddsperspektiv.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**. Vi noterade ett antal förbättringsmöjligheter avseende styrning av informations- och IT-säkerheten.

PwC rekommenderar kommunstyrelsen att:

- Intensifiera arbetet med att utveckla befintlig systemförvaltningsmodell med fokus på att förankra informationssäkerhetsrelaterade ansvarsområden i verksamheterna och för definierade roller.

Fortsättning nästa sida

.

3. Resultat av granskning

3.1 Revisionsfråga 1: *Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?*

Forts.

- Säkerställa att verksamheterna organiserar sig unisont inom deras arbete med informationssäkerhet för att få genomslag och synergier av varandras informationssäkerhetsarbete.

- Säkerställa att ansvariga inom området har tillräckligt med resurser och mandat för att bedriva ett ändamålsenligt informationssäkerhetsarbete enligt framtagna riktlinjer, systemförvaltningsmodell och således vidtar tillräckliga åtgärder för att upprätthålla säkerhet inom deras respektive enheter.

.

3. Resultat av granskning

3.2Revisionsfråga 2: Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?

Iakttagelser

Danderyds kommun har ett antal styrande dokument som ligger till grund för informationssäkerhetsarbetet och följer en tydlig dokumentationshiearki. Utformningen på dokumentationen är sprunget utifrån informationssäkerhetsstandarden ISO 27001. Dokumentationen utgår från en övergripande informationssäkerhetspolicy satt av kommunfullmäktige. Vidare finns tillhörande och kompletterande riktlinjer och anvisningar för informationssäkerhet som beskriver mer i detalj hur arbetet skall utformas på operativ nivå.

Det är kommunens informationssäkerhetssamordnare som driver arbetet med att framställa styrande dokumentation. Under granskningen noterades dock att en tydlig rutin för när och hur kommunen skall arbeta med riskanalys saknas, vilket är en central aktivitet i ett ledningssystem för informationssäkerhet.

Dokumentationen finns tillgänglig på kommunens intranät, under granskningen framkom dock att kännedomen om dokumentationens existens bland anställda är låg. Det framgår även under intervjuer att det saknas ett etablerat arbetssätt att följa upp hur organisationen efterlever framtagna styrdokument. Säkerhetsavdelningen har ingen rutin för att genomföra kontrollinsatser eller stickkontroller i syfte att bedöma följsamhet, Vidare noterades även att det inom kommunens internkontroll saknas kontrollmoment med hänsyn taget till informationssäkerhet. Således saknas en grund för en samlad bedömning över huruvida informationssäkerhetsdokumentation är väl implementerad i verksamheten.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**. Policys och instruktioner saknar förankring och återspeglar inte i alla delar hur kommunen faktiskt arbetar med informationssäkerhet. PwC noterade ett antal förbättringsmöjligheter, följande rekommendationer lämnas mot bakgrund till iakttagelserna:

PwC rekommenderar kommunstyrelsen att:

- Öka medvetenheten gällande de styrande dokumenten och sprida kunskaper om deras innehåll med fokus på implementering och efterlevnad.
- Förankra innehåll i framtagna styrande dokument i syfte att skapa rätt förutsättningar för efterlevnad av styrande dokumentation, instruktioner och rutiner.
- Ta fram genomförandeplan för hur efterlevnad av riktlinjer för medarbetare ska säkerställas.
- Formalisera och utvärdera möjlighet att inkludera regelbundet återkommande arbetsmoment och kontroller mht IT- och informationssäkerhet i som en del av övriga internkontrollplaner samt systemförvaltningsplaner.
- Prioritera fastställande av framtagna styrande dokumentation för informations- och IT-säkerhet och säkerställa att de regelbundet följs upp och vid behov revideras.

3. Resultat av granskning

3.3 Revisionsfråga 3: *Finns ett ledningssystem för informationssäkerhet implementerat?*

Iaktagelser

Kommunfullmäktige har antagit flera styrande dokument inom ramen för kommunens informationssäkerhetsarbete men saknar i dagsläget ett heltäckande ledningssystem för informationssäkerhet. Under granskningen noterades att ett antal nyckelprocesser som bör genomföras inom ramen för ett ledningssystem saknas. Exempel på detta är att arbetet med informationsklassificering samt genomförande av riskanalyser med fokus på informationssäkerhet är eftersatt.

För att säkerställa att ändamålsenlig säkerhet upprätthålls för kommunens verksamhet, oavsett om den bedrivs i egen regi eller av leverantör framgår det i styrande dokumentation att säkerhetsåtgärder alltid ska vidtas i samband med upphandling. Detta inkluderar att alltid inkludera säkerhetsenheten under upphandling. Det framkom dock under granskningen att detta inte alltid görs. Vidare noterades att det saknas rutiner för uppföljning som säkerställer att leverantörer uppfyller grundläggande säkerhetsåtgärder såsom; återläsning av säkerhetskopior, verifiering och test av dataåterställningsplaner, genomförande av sårbarhetsskanning etc. Detta kan förslagsvis hanteras och inkluderas som ett kontrollmoment i ett årshjul med hänsyn till IT och informationssäkerhet.

Mot bakgrund i en avsaknad av ett tydligt definierat LIS saknas det även tydlig övervakning och mätning (efterlevnad) av informationssäkerhetsarbetet, riskhanteringsarbete och beslutade säkerhetsåtgärder. PwC noterade att befintliga aktiviteter och säkerhetsåtgärder som finns implementerade inte utvärderas mot avsedd verkan och att de fungerar tillfredsställande. Detta inkluderar även processen att inkludera högsta ledningen årligen för att ge en statusbild av arbetet med informationssäkerhet.

Per intervjuer har granskningen visat att kommunen nyligen har initierat ett arbete med att att ta fram kontinuitets- och beredskapsplaner. Avsaknaden av dessa planer återspeglades i det faktum att verksamheterna idag inte arbetar aktivt med att ta kravställa mot IT-avdelningen utifrån perspektiven konfidentialitet, riktighet och tillgänglighet. Istället är det IT som tolkar verksamheterna behov. Ett sådant arbetsflöde är inte önskvärt då det är verksamheterna som bör härleda verksamhetens krav på tillgänglighet, konfidentialitet och riktighet och således härleda korrekta krav på informationen och dess skyddsvärde.

Under intervju beskrivs det att backuper regelbundet tas samt att IT gör slumpmässigt utvalda återläsningstest regelbundet i syfte att avgöra om backuphanteringen är ändamålsenliga.

Fortsättning nästa sida

3. Resultat av granskning

3.3 Revisionsfråga 3: *Finns ett ledningssystem för informationssäkerhet implementerat?*

Forts.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld** då kommunen i nuläget inte har en tillräcklig nivå gällande ledningssystem för informationssäkerhet samt att kommunen saknar ett systematiskt uppföljningsarbete vad gäller arbetet med informationssäkerhet både på förvaltnings, samt kommunledningsnivå. PwC rekommenderar kommunstyrelsen att:

- Intensifiera genomförande av mer omfattande riskanalys på systemnivå med bäring på IT- och informationssäkerhet. Det är förvaltningarna som ska ha ansvaret för att driva identifieringen av risker och de informationstillgångar som är relevanta att skydda, men att centrala funktioner tillhandahåller nödvändig resurser, mandat och tydliga roller för att stödja dess genomförande.I detta ingår att definiera kriterier för riskacceptens kommunen.

- Säkerställa att riskhanteringsåtgärder har en ansvarig person utsedd, tidsram, finansiering och uppföljning i syfte att begränsa risker och uppfylla skyddskrav.

- Utveckla övergripande kontinuitetsplan för att säkerställa att verksamheten har effektiva processer, system och stöd för att motverka långvariga avbrott i verksamheten. Kontinuitetsplan kan ses som kravställare till IT-avdelningen och andra samarbetspartners vid utformning av avbrottsplan.

- Fastställa vad som för kommunen är verksamhetskritiska system samt att påbörja klassificering av detsamma. Vidare rekommenderas kommunen att framställa och dokumentera metod för klassificering i styrande dokumentation. Det är av vikt att ha kännedom om vilka system som är kritiska för verksamheten för att bland annat kunna kravställa vad outsourcingsleverantörer ska prestera samt för att fastställa ändamålsenliga informationssäkerhetskrav i befintliga och kommande avtal.

- Utveckla avbrottsplaner, innefattande hur allvarliga avbrottssituationer ska hanteras och nödvändiga åtgärder för att få tillbaka IT-stödet enligt verksamhetens krav, samt testa planen regelbundet.

- Utvärdera ifall det finns behov av att ta in oberoende tredjepart för att verifiera och säkerställa att informationssäkerhetskrav som ställs i avtalen för kritiska systemleverantörer är ändamålsenliga.

- Ta fram rutin att inkludera kommunledningen årligen i hur det fortlöpande arbetet med informationssäkerhet fortskrider.

3. Resultat av granskning

3.4 Revisionsfråga 4: *Sker kommunens arbete med informationssäkerhet systematiskt?*

Iaktagelser

I riktlinjen för informationssäkerhet framgår det att anställda genomgår utbildning vid nyanställning samt vid återkommande intervall. Det specificeras dock inte ytterligare hur arbetet ska bedrivas eller vem som bär ansvaret för att säkerställa att riktlinjen efterlevs. Under granskningen noterades att det är informationssäkerhetssamordnaren som ansvarar för att ta fram säkerherhetsutbildningar. Exempelvis används kommunens intranät för att sprida kunskap i form av nyhetsutskick samt extra e-utbildningar inom informationssäkerhet för att öka organisationens kunskap.

Kommunen använder sig av även av plattformen Junglemaps i syfte att tillhandahålla anställda nano-utbildningar inom informationssäkerhet. Framtagen nano-utbildningen är obligatorisk och skall ha genomgåtts av alla kommunens anställda samt politiskt valda under våren, granskningen visar dock att enbart 60% fullföljde utbildningen.

Kommunen saknar i dagsläget metoder för riskhantering vilket omfattar risk-och sårbarhetsanalyser samt informatoinsklsasificering. Arbetet med att färdigställa informationsklassificeringar, både för kommungemensamma och verksamhetsspecifika system, har ännu inte färdigställts.

Slutligen noterades att det i dagsläget inte finns en acceptabel risknivå som i förhållande till IT- och informationssäkerhetsrisker varken mot kommunstyrelsen eller mot kritiska samarbetspartner i förhållande till teknisk infrastruktur.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld.** Kommunstyrelsen har i nuläget endast delvis tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot. Riskanalyser för informationsrisker, kontinuitetsplaner och avbrottsplaner bör färdigställas för samtliga förvaltningar och deras tillhörande kritiska system. Följande rekommendationer lämnas mot bakgrund till iakttagelserna. Vad gäller utbildning finns en tydlig plan inom ramen för informationssäkerhet samt säkerhetsmedvetenhet. Däremot är nivån av deltagande inte tillräckligt hög för att insatserna skall anses som ändamålsenliga.

Vi rekommenderar kommunstyrelsen att;

- Införa tydlighet kring obligatoriska, regelbundna utbildningsmoment för samtliga medarbetare. Utbildningarna bör utgå från ett informationssäkerhetsperspektiv och inte vara sprunget ur ett GDPR-hänseende.
- Intensifiera arbetet med att rulla ut mikroutbildningar till samtliga medarbetare inom cybersäkerhetsrelaterade riskområden.
- Genomför incidentövningar för prioriterade hot som beskriver roller, ansvar och aktiviteter i syfte att öka förmågan att effektivt reagera och hantera en storskalig IT-incident.
- Systematisera arbetet med olika samverkansforum inom kommunen för att sprida kunskap och erfarenheter.

4

Samlad bedömning

4. Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Danderyds kommun genomfört en granskning av informationssäkerhet. Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelsen **inte helt** säkerställer ett ändamålsenligt informationssäkerhetsarbete och att detta sker med tillräcklig intern kontroll. Bedömningen baseras på utfallet av nedan revisionsfrågor:

Revisionsfråga	Bedömning
1. *Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?*	**Delvis** *Det blir tydligt under intervjuerna att även om det finns en tydlig roll- och ansvarsfördelning gällande kommunens informationssäkerhetsarbete på centralt håll saknas det en förankring i verksamheten som säkerställer efterlevnad av framtagna riktlinjer.*
2. *Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?*	**Delvis** *Det finns ett antal styrande dokument som i sig anses vara ändamålsenliga. Dock behöver de styrande dokumenten nå ut och förankras ändamålsenligt ute i verksamheten.Policys och instruktioner saknar förankring och återspeglar inte i alla delar hur kommunen faktiskt arbetar med informationssäkerhet*.
3. *Finns ett ledningssystem för informationssäkerhet implementerat?*	**Delvis** *Det saknas i dagsläget ett komplett ledningssystem för informationssäkerhet. Det finns styrande dokumentation men flera nyckelaktiviteter görs inte systematiskt såsom informationsklassning och riskanalys. Vidare saknas det i dagsläget ett systematiskt uppföljningsarbete vad gäller arbetet med informationssäkerhet både på förvaltnings, samt kommunledningsnivå.*
4. *Sker kommunens arbete med informationssäkerhet systematiskt?*	**Delvis** *Det finns i dagsläget aktiviteter framtagna i syfte att uppnå systematik i det löpande arbetet i form av utbildningar för anställda och olika forum för kunskapsdelning inom organisationen. Dock är en del av dessa forum pausade vilket påverkar systematiken negativt. Vidare saknar heltäckande rutiner för att identifiera och hantera risker oh hot. Riskanalyser för informationsrisker, kontinuitetsplaner och avbrottsplaner bör färdigställas för samtliga förvaltningar och tillhörande verksamhetskritiska system.*

5

Bilaga

Bilaga A - Dokumentationslista

5. Bilaga A - Dokumentationslista

Dokument	Diarienummer	Beslutad	Reviderad
Riktlinjer för säkerhet	KS 2021/0213		2021-05-24
Rutin för informationsklassning	KS 2020/0051	2020-01-09	
Rutin e-post	KS 2022/0139		2022-02-23
Anvisning organisation för säkerhet och dataskydd	KS 2021/0474		2021-12-01
Anvisning säkerhet	KS 2020/0051		2020-01-10
It-säkerhet för användare		2020-06-03	
Policy för informationssäkerhet och dataskydd	KS 2019/0428		2021-03-22
Systemförvaltningsmodell	KS 2020/0347		2020-08-17

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Danderyd kommuns förtroendevalda revisorer enligt de villkor och under de förutsättningar som framgår av beslutad projektplan. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.

2022-10-26

Kristian Damlin

_____

Uppdragsledare

pwc.com