Informations-säkerhetsgranskning

Söderköpings kommun

PwC Sverige
2022

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Söderköpings 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.

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?	**Nej**	
Finns styrande informationssäkerhetsriktlinjer och är dessa implementerade i verksamheten?	**Delvis**	
Finns ett ledningssystem för informationssäkerhet implementerat?	**Nej**	
Bedriver informationssäkerhetsorganisationen ett aktivt informationssäkerhetsarbete?	**Nej**	
Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet i verksamheterna?	**Nej**	

Rekommendationer

Mot bakgrund av vad som framkommit i granskningen lämnas följande rekommendationer:

- Tydliggör roll- och ansvarsfördelning samt säkerställ att dessa har tillräckligt med resurser och mandat. Kommunen bör se över resurssituationen och säkerställa att det finns tillräckliga resurser för att bedriva ett ändamålsenligt informationssäkerhetsarbete.
- Kommunen bör fastställa en färdplan för införandet av ett ledningssystem för informationssäkerhet. En sådan färdplan bör innehålla tydliga målsättningar, ansvarsbeskrivningar för medverkande resurser, samt en konkret tidsram som arbetet för framtagning av ett ledningssystem ska förhålla sig till.
- Kommunen bör utreda möjligheten att upprätta en arbetsgrupp för informationssäkerhet som sammanträder regelbundet och inkluderar nyckelpersoner för arbetet. Denna grupp bör ha ansvar för förvaltning av ledningssystemet för informationssäkerhet och bör ha som uppgift att styra och samordna informationssäkerhetsarbetet inom hela kommunen. Arbetsgruppen bör vidare ha ett övergripande ansvar för omvärldsbevakning inom informationssäkerhetsområdet.

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.

- Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Söderköpings kommun. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet

- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Kommunen bör genomföra systematiska uppföljningar av utbildningsverksamheten.

- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.

- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

- Kommunen bör se över förvaltningsmodellen för verksamhetssystem och utreda möjligheter till att förstärka ansvaret som systemägare har för tillämpning av informationssäkerhetsåtgärder.

Innehållsförteckning

Inledning

Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag. Detta då 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 i sin tur skapar förtroende både inom och utanför organisationen.

Revisorerna har i sin riskanalys för 2020 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.

Revisionsfrågor:

1. Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
2. Finns styrande informationssäkerhetsriktlinjer och är dessa implementerade i verksamheten?
3. Finns ett ledningssystem för informationssäkerhet implementerat?
4. Bedriver informationssäkerhetsorganisationen ett aktivt informationssäkerhetsarbete?
5. Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet i verksamheterna?

Revisionskriterier

- Kommunallagen
- IT-Styrdokument
- Informationssäkerhetsdokumentation

Avgränsning

I tid avgränsas granskningen till år 2021 samt till granskningens revisionsfrågor.

Metod

Granskningen genomförs med hjälp av intervjuer av identifierade nyckelpersoner i kommunen, samt inläsning och genomgång av tillgänglig dokumentation.

De funktioner som intervjuats inom ramen för granskningen är följande:

- Kanslichef / säkerhetschef / säkerhetsskyddschef
- Säkerhetssamordnare / beredskapssamordnare / signalskyddschef
- IT- och digitaliseringschef
- Kommunstyrelsens ordförande

Granskningsresultat

1.1 Revisionsfråga 1

Finns en tydlig informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?

Iakttagelser

I Söderköpings kommun finns en IT-avdelning och en säkerhetsavdelning som tillsammans arbetar med kommunens informationssäkerhet. Ansvarig för säkerhetsavdelningen är kanslichefen som är tillika säkerhetsskyddschef. Det framkommer i intervjuer att ansvaret för informationssäkerheten tidigare legat på IT-avdelningen, men att ansvaret delvis flyttats över till säkerhetsavdelningen under hösten 2019. Det har dock enligt intervjuer inte skett någon formell överlämning, vilket resulterat i att det finns en osäkerhet kring gällande roller, mandat och ansvar för informationssäkerhetsarbete både hos IT-avdelningen och säkerhetsavdelningen. Fram till 2019 fanns en informationssäkerhetssamordnare i kommunen, sedan dess saknas en funktion som dedikerat arbetar med informationssäkerhet.

I kommunens säkerhetsavdelningen finns det i dagsläget två personer som ska arbeta med informationssäkerhet, säkerhetssamordnaren och säkerhetsskyddschefen, tillika kanslichefen. Enligt intervjuer saknas det en tydlig kravställan från kommunstyrelsen gällande vad som ska innefattas i informationssäkerhetsarbetet och dess organisation. IT-avdelningen ansvarar enligt intervjusvar för IT-arkitektur, drift och säkerhet. Däremot saknas det även här en tydlig kravställan för hur detta ansvar ser ut. Den fysiska säkerheten i kommunen sköts till största del av Fastighetskontoret, som ansvar för den fysiska säkerheten i kommunens lokaler.

Samtliga av kommunens verksamheter har en lagstadgad skyldighet att ta fram en risk- och sårbarhetsanalys (RSA) i enlighet med lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Inom ramen för verksamheternas RSA kan informationssäkerhetsrelaterade risker identifieras. Utöver RSA identifieras inga risker och de informationssäkerhetsrelaterade risker som identifieras i verksamheternas risk- och sårbarhetsanalyser aggregeras inte vidare separat för att säkerställa att kommunen i sin helhet kan hantera eller bearbeta dessa.

Under intervjuerna framgår det att de som idag arbetar med informationssäkerhetsarbetet saknar resurser och mandat. Detta är enligt utsago en konsekvens av den omorganisation som genomfördes under 2019. Det styrdokument som idag finns avspeglar inte den nuvarande organisationen. Dokumenten som finns idag bygger snarare på den struktur som gällde när ansvaret låg under IT-avdelningen.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att revisionsfrågan är **ej uppfylld.**

Det framkommer under intervjuerna att det finns en avsaknad av en tydlig roll- och ansvarsfördelning gällande kommunens informationssäkerhetsarbete. Vidare saknas det i dagsläget en kravställan för informationssäkerhet, vilket försvårar förutsättningarna för att bedriva ett ändamålsenligt informationssäkerhetsarbete. Det framkommer även att det finns begränsade resurser i förhållande till det arbete som behöver göras inom ramen för informationssäkerhetsarbetet. Detta resulterar i att de funktioner som arbetar med informationssäkerhet endast har möjlighet att göra det absolut nödvändiga, snarare än det arbete som krävs för att upprätta en ändamålsenlig informationssäkerhet i kommunen och dess verksamheter.

1.2 Revisionsfråga 2

Finns styrande informationssäkerhetsriktlinjer och är dessa implementerade i verksamheten?

Iakttagelser

Söderköpings kommun har ett antal styrande dokument för informationssäkerhet i form av en infomationssäkerhetsplan, en IT-plan, riktlinjer för kontroll av IT-utrustning samt två informationssäkerhetsinstruktioner; en för användare och en för förvaltning och drift. I informationssäkerhetsplanen framgår att den innehåller Söderköpings kommuns övergripande mål för informationssäkerhetsarbetet. Det framgår även att samtliga nämnder och deras verksamheter omfattas av informationssäkerhetsplanen. Utöver det formaliseras kommunens övergripande målsättning samt strategiska målområden i informationssäkerhetsplanen. Dokumentationshierarkin ser enligt kommunens informationssäkerhetsinstruktion för förvaltning och drift ut som nedan.

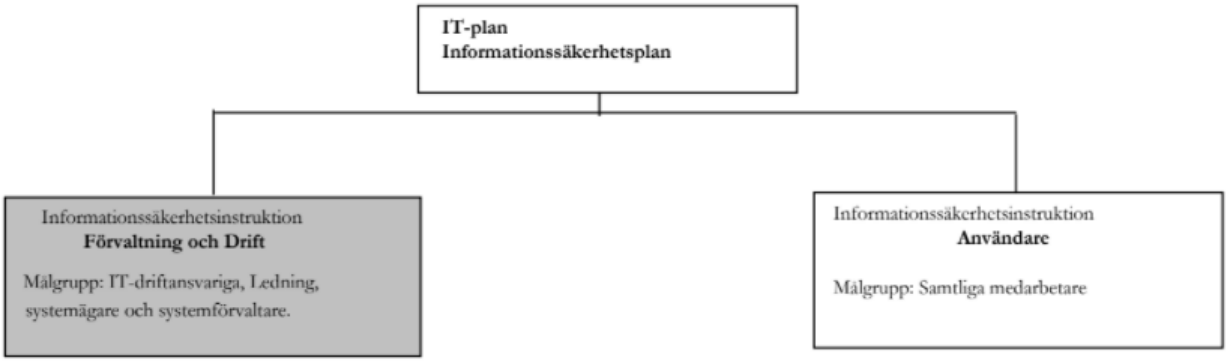

Bild 1. Från *Informationssäkerhetsinstruktion förvaltning och drift 2018-2022*

Dokumentationen togs fram av kommunens IT-avdelning under tiden det fanns en informationssäkerhetssamordnare. Sedan dokumentens framtagning har, som tidigare nämnt, ansvaret flyttats från IT-avdelningen samt att inte längre finns någon informationssäkerhetssamordnare. Till följd av detta framkommer i intervjuer att mycket av dokumentationens innehåll inte längre överensstämmer med informationssäkerhetsarbetet i praktiken. Det framgår även att inga aktiviteter har genomförts sedan 2019 för att implementera dokumentationens innehåll eller för att säkerställa att identifierade målsättningar och målområden uppfylls. Detta beskrivs i intervjuer vara ett resultat av bland annat en osäkerhet kring roller, ansvar samt begränsade resurser. Det framkommer även i intervjuer att det saknas rutiner för hur dokument ska implementeras när de är beslutade för att säkerställa dess efterlevnad.

I den befintliga dokumentationen framgår tydligt giltighetstid samt när den senast reviderades. Samtliga dokument är även beslutade och har diarienummer. Då giltighetstiden för samtliga informationssäkerhetsrelaterade dokument går ut under 2022 konstateras det i intervjuer att det under 2022 kommer behöva ske ett arbete med att utveckla ny dokumentation som är baserad på den befintliga organisationen.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**.

Det kan konstateras att Söderköpings kommuns befintliga informationssäkerhetsdokumentation kan anses vara ändamålsenlig, framförallt baserat på dess innehåll. Däremot framgår det tydligt under granskningens gång att det finns en tydlig diskrepans mellan dokumentationen och arbetet

i praktiken, framförallt till följd av att ansvar och roller bytts ut samt att det tydligt konstateras att det som framgår i dokumentationen inte efterlevs. Baserat på intervjusvar framhålls även tydligt att dokumentationen inte är implementerad i kommunens verksamhet och att det saknas rutiner och processer för att implementera den styrande dokumentationen.

Söderköpings kommun saknar dokumentation för flera processer med bäring på ett strukturerat informationssäkerhetsarbete. Avseende exempelvis riskhantering, som är en viktig del av informationssäkerhet, noteras att det saknas både formell dokumentation samt befintligt arbete. Det saknas även dokumentation som fastställer kommunens riskaptit eller risktolerans som eventuella riskhanteringsåtgärder bör förhålla sig till.

Det kan vidare konstateras att Söderköpings kommun inte arbetar aktivt med rutiner och processer med syfte att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle inkludera implementation av dokumentationen vid exempelvis nyanställning.

Bedömningen är sammanfattningsvis således grundad i avsaknaden av implementation av dokumentationen samt den tydliga diskrepansen mellan dokumentation och hur arbetet sker i praktiken, iakttagelsen att vissa processer saknar dokumentation, samt i iakttagelsen att det saknas ett strukturerat ledningsarbete som definierar samordningen gällande samtlig väsentlig dokumentation.

1.3 Revisionsfråga 3

Finns ett ledningssystem för informationssäkerhet implementerat?

Iakttagelser

Söderköping kommun har som tidigare nämnts ett antal styrande dokument inom ramen för informationssäkerhet. Det framgår i intervjuer att funktioner från Söderköping besökt en annan närliggande kommun för att undersöka kommunens ledningssystem för informationssäkerhet. Under 2022 planerar Söderköpings kommun att anamma delar av detta för att stärka det egna informationssäkerhetsarbetet.

Sedan 2019 genomför inte kommunen någon informationsklassning i samband med att den tidigare informationssäkerhetssamordnaren slutade. Vidare saknar kommunen en process för att prioritera eller klassificera tillgångar och resurser. Arbetsprocessen genomförs istället genom att incidenter prioriteras utifrån person, förvaltning eller kommunnivå. Enligt intervjuer finns det muntliga och informella prioriteringsordningar.

Kommunen genomför inte några riskanalyser kopplade till IT- eller informationssäkerhet utöver det som framkommer i verksamheternas risk- och sårbarhetsanalyser. Enligt intervjuer finns det en tydlig avsaknad av systematik kopplat till riskanalyser, konsekvensanalyser och sårbarhetsanalyser vid exempelvis upphandlingar. Under intervjuer framgår det att det är projektledaren för respektive upphandling som beslutar vilka funktioner som medverkar, vilka analyser som görs samt vilka krav som ställs på leverantörer.

Söderköpings kommuns incidenthantering baseras i dagsläget till stor del på informella rutiner. Det som framgår i styrande dokument efterlevs enligt intervjuer inte. Vidare saknas det i en tydlig definition av vad som utgör en informationssäkerhetsincident samt hur denna ska rapporteras. När en incident inträffar meddelas berörda via antingen e-post eller telefon. Det saknas även en tydlig roll- och ansvarsfördelning under incidenthanteringen. Kommunen har enligt intervjuer inte något dokumenterad incidentplan, utan delar av incidenthanteringen beskrivs i *Informationssäkerhetsinstruktion förvaltning och drift 2018-2022*.

Lärdomar och mönster från inträffade incidenter förmedlas till berörda verksamheter på verksamhetens arbetsplatsträff. Där tas incidenten upp och sedan beskrivs eventuella

förändringar i rutiner eller arbetssätt som identifierats för att förhindra eventuella liknande incidenter. Däremot framkommer det under intervjuer att det saknas formella rutiner för hur och när detta ska göras, utan det som sker i dagsläget är på enskilda anställdas initiativ.

Den dataskyddsteknik som Söderköpings kommun använder är till största del logghantering, både i brandvägg och på domänkontrollanter. Vidare finns det ett antal regler i kommunens brandvägg för att reglera vad som ska släppas in respektive stängas ute. Brandväggen används även för att förhindra exekverbara mail och filer. Blockering av USB-portar är implementerat i kommunens hårdvaror, för att exempelvis göra det svårare för eventuella antagonister och andra oönskade besökare att invadera datorn med skadlig programvara via den fysiska USB-porten. Vidare har kommunen enligt intervjuer även segmenterat sina nätverk i bland annat ett teknikernät och ett mobilnät. Intervjusvar uppger att säkerhetskopiering sker regelbundet, men att backuper endast lagras på en fysisk plats.

Bedömning
Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att revisionsfrågan är **ej uppfylld**.

Söderköpings kommun har i dagsläget inte ett ledningssystem för informationssäkerhet. Det finns, som tidigare nämnt, ett antal styrande dokument på plats. Däremot finns en tydlig avsaknad av systematik som präglar kommunens informationssäkerhetsarbete i form av incidenthantering, organisation, dokumentation, uppföljning och kontroll. Under intervjuerna framgår det att det finns en tydlig avsaknad av roll- och ansvarsfördelning och en otydlig struktur för förvaltning av system. Det konstateras även finnas en tydlig begränsningar gällande befintliga resurser inom ramen för informationssäkerhetsarbetet. Det finns en medvetenhet om att det återstår mycket arbete inom detta projekt och att det i nuläget saknas en mogen organisatorisk struktur som kan ta emot och förvalta ledningssystemet.

1.4 Revisionsfråga 4
Bedriver informationssäkerhetsorganisationen ett aktivt informationssäkerhetsarbete?

Iakttagelser
Det framgår i *Informationssäkerhetsinstruktion förvaltning och drift 2018-2022* att det är informationssäkerhetssamordnaren som ska stödja arbetet med att uppnå informationssäkerhetsplanens mål samt som ansvarar för analyser av de delar av IT-stödet som är gemensamt för hela verksamheten med stöd av KLASSA. Vidare framgår att det även är informationssäkerhetssamordnaren som stödjer systemägarnas arbete med att genomföra enskilda systemsäkerhetsanalyser samt som ansvarar för sammanställning av beslutsunderlag om införande av informationssystemet i kommunen. Slutligen står det även uttryckligen att det är informationssäkerhetssamordnaren som ska sammanställa och rapportera följande till ledningen:

- intrång och försök till intrång
- brott mot lagstiftning och internt regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång eller funktionsfel.

Då det som tidigare nämnt inte funnits någon informationssäkerhetssamordnare sedan 2019 har inget av det ovan nämnda genomförts sedan dess. Det framgår i intervjuer att det finns en osäkerhet kring rådande ansvar, ansvarsfördelning, roller och beslut gällande informationssäkerhetsarbetet.

Det saknas ett dedikerat samverkansforum där relevanta funktioner från kommunen har möjlighet att delta. Delar av kommunens säkerhetsavdelning medverkar i ett samverkansforum som SKR (Sveriges Kommuner och Regioner) anordnar där IT diskuteras frekvent, däremot inte informationssäkerhet specifikt. Vidare finns även ett annat säkerhetsnätverk som Länsstyrelsen anordnar där frågor rörande informationssäkerhet kan diskuteras, dock ligger fokus framförallt på områden som signalskydd och säkerhetsskydd.

I dagsläget sker inget arbete för att säkerställa att förvaltningar och bolag i kommunen skyddar sina system på ett adekvat sätt samt kravställer gentemot IT. Vidare har det inte etablerats någon nivå av säkerhet som kommunens bolag eller förvaltningar ska efterföljas. Det sker ingen uppföljning eller intern kontroll av detta utöver genomgång av de risk- och sårbarhetsanalyser som verksamheterna rapporterar in. Under 2022 kommer en kommungemensam förvaltningsmodell för förvaltning av verksamhetssystem tas fram som planeras vara klart till årsskiftet 2022/2023.

Informationsklassning genomförs inte i någon av kommunens verksamheter i dagsläget. Det har tidigare genomförts av kommunens informationssäkerhetssamordnare, men sedan denna funktion försvann 2019 har arbetet inte upprätthållits. Detta har resulterat i att informationsklassning inte genomförs, dokumenteras eller kommuniceras, exempelvis gällande kommunens kritiska system. Det framgår av intervjusvar att erfarenhetsåterföring, och utvärderingar, exempelvis i form av ny lagstiftning, incidenter, omvärldsbevakning eller i det löpande arbetet, inte genomförs i önskad utsträckning.

Utifrån intervjuer med ledande beslutsfattare inom kommunen har det framkommit att rapportering till kommunstyrelsen avseende informationssäkerhets- händelser, incidenter samt övriga områden som berör informationsförvaltning inte sker. Det framkommer även att det inte är något som efterfrågas av kommunstyrelsen.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att revisionsfrågan är **ej uppfylld**.

Det kan konstateras att Söderköpings kommun inte arbetar aktivt med rutiner och processer med syfte att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle bland annat inkludera regelbunden revision och uppdatering av styrande dokument för att säkerställa att de är väl implementerade i kommunens verksamheter och överensstämmer med organisation, roller och ansvar.

1.5 Revisionsfråga 5

Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet i verksamheterna?

Iakttagelser

Söderköpings kommun saknar enligt intervjuer i dagsläget en informationssäkerhetsutbildning för kommunens anställda. Vid nyanställning tillhandahålls ett kompendium där det står ett fåtal rader om informationssäkerhet där det framgår vikten utav det. Enligt intervjusvar är det kommunens chefer som ansvarar för att upplysa nyanställda om vad som finns inom området. På kommunens intranät finns en flik om informationssäkerhet där det hänvisas till Myndigheten för samhällsskydd och beredskaps (MSB) utbildning Digital informationssäkerhetsutbildning för alla (DISA). Däremot går det inte att spåra eller följa upp vilka som gått denna utbildning. Det framkommer i intervjuer att det finns önskemål om att implementera denna utbildning som en obligatorisk del i onboarding-processen för nyanställda. När kommunstyrelsen tillträdde fick de genomgå en kortare informationssäkerhetsutbildning, det har dock inte skett någon uppföljning av denna.

Kommunen bedriver inga övningar kopplat till informationssäkerhet. Det framgår under intervjuer att förståelsen för informationssäkerheten är generellt låg hos kommunens anställda. Däremot är säkerhetsmedveten något högre i vissa delar av kommunens verksamhet, exempelvis Socialtjänsten, som regelbundet hanterar känsliga och sekretessbelagda uppgifter inom ramen för sitt arbete och uppdrag. I dokumentet *Informationssäkerhetsinstruktion för användare i Söderköpings kommun* finns riktlinjer och rutiner för hur medarbetare bör hantera sin utrustning samt vad som bör göras om en anställd lämnar sin arbetsplats. Det konstateras dock utifrån intervjusvar att det som framgår ofta inte efterlevs i praktiken.

Kommunen har informationshanteringsplaner som bland annat beskriver tillvägagångssätt för arkivering. Informationshanteringsplanerna är enligt intervjusvar sammanställningar över de allmänna handlingarna som återfinns inom en myndighet och beskriver hur de ska hanteras i fråga om exempelvis registrering, bevarande, gallring och arkivering. Under 2021 togs en ny mall fram för informationshanteringsplanerna baserat på den processbaserade klassificeringsstruktur som kommunen använder sig av vid registrering av allmänna handlingar. Mallen introduceras löpande i kommunens verksamheter vid framtagande av nya informationshanteringsplaner och vid revidering av gamla. I den nya mallen finns det med en rubrik för att även informationsklassa de handlingstyper som beskrivs i planen. Det är dock i dagsläget endast en verksamhet som använt sig av den nya modellen, men enligt intervjusvar introduceras den som tidigare nämnt löpande allt eftersom informationshanteringsplanerna revideras. Enligt intervjusvar framkommer även att det finns en utmaning i att få samtliga planer uppdaterade efter den nya modellen samt att få kommunens verksamheter att prioritera detta arbete till följd av flertalet pågående initiativ.

Utöver ovan nämnda saknas det i övrigt rutiner för hur dokument ska klassificeras. Gällande fysisk säkerhet finns det muntliga instruktioner för hur besökshantering ska genomföras inne i kommunens lokaler. En obehörig får enligt intervjuer aldrig röra sig fritt i lokalerna och måste hämtas upp i receptionen av en kommunanställd. Alla anställda ska alltid bära sitt passerkort synligt så att det är enkelt att urskilja vem som är behörig och obehörig.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att revisionsfrågan är **ej uppfylld.**

I Söderköpings kommun finns i dagsläget inget aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet. Under intervjuer framgår det att det finns en tydlig avsaknad av utbildningar och övningar inom ramen för informationssäkerhet samt säkerhetsmedvetenhet i allmänhet.

Som ett led i att förhindra cybersäkerhetsincidenter och upprätthålla samhällsviktig verksamhet behöver en kommun bedriva ett ändamålsenligt informationssäkerhetsarbete. Information som finns i kommunen skall klassas, rutiner och riktlinjer ska finnas på plats och arbetet ska regelbundet följas upp. Detta kräver också ett säkerhetsmedvetande hos dem som hanterar informationen på daglig basis. Informationssäkerhet regleras inte i en sammanhållande lag utan genom bestämmelser i flera olika regelverk. Att kommunstyrelsen inte efterfrågar rapportering gällande informationssäkerhet resulterar i att medvetenheten om informationssäkerhet inte kan säkerställas.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Söderköpings 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?*	**Nej** Det blir tydligt under intervjuerna att det finns en stor avsaknad av en tydlig roll- och ansvarsfördelning gällande kommunens informationssäkerhetsarbete. Vidare saknas det en kravställande kopplat till informationssäkerhet, vilket försvårar utförandet och förutsättningarna för att kunna bedriva informationssäkerhetsarbetet. Det kan även konstateras att det finns begränsat med resurser för att kunna bedriva ett ändamålsenligt informationssäkerhetsarbete.	
2. *Finns styrande informationssäkerhetsriktlinjer och är dessa implementerade i verksamheten?*	**Delvis** Söderköpings kommun har ett antal styrande dokument som i sig anses vara ändamålsenliga. Dock konstateras det under granskningen att dessa inte överensstämmer med verkligheten, framförallt till följd av att ansvar och roller bytts ut, samt att dokumentationen till stor del inte efterlevs.	
3. *Finns ett ledningssystem för informationssäkerhet implementerat?*	**Nej** Söderköpings kommun har i dagsläget inte ett ledningssystem för informationshantering. Det finns styrande dokumentation för området, men det saknas en genomgående systematik i informationssäkerhetsarbetet. Vidare saknas det en tydlig roll- och ansvarsfördelning.	
4. *Bedriver informationssäkerhetsorganisationen ett aktivt informationssäkerhetsarbete?*	**Nej** Söderköpings kommun arbetar inte aktivt med rutiner och processer i syfte att fortsätta utveckla och stärka processer gällande arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle	

	inludera regelbunden revision och uppdatering av styrande dokument för att säkerställa att de är väl implementerade i kommunens verksamheter och överensstämmer med organisation, roller och ansvar.	
5. *Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet i verksamheterna?*	**Nej** I Söderköpings kommun finns i dagsläget inget aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet. Det bedrivs inga obligatoriska utbildningar eller övningar i informationssäkerhet. Kommunstyrelsen har genomgått en utbildning i informationssäkerhet vid mandatperiodens början, men ingen uppföljning av denna har skett. Vidare framkommer i intervjuer att säkerhetsmedvetenheten hos kommunens anställda generellt sett anses vara låg.	

Rekommendationer

Mot bakgrund av vad som framkommit i granskningen lämnas följande rekommendationer:

- Tydliggör roll- och ansvarsfördelning samt säkerställ att dessa har tillräckligt med resurser och mandat. Kommunen bör se över resurssituationen och säkerställa att det finns tillräckliga resurser för att bedriva ett ändamålsenligt informationssäkerhetsarbete.
- Kommunen bör fastställa en färdplan för införandet av ett ledningssystem för informationssäkerhet. En sådan färdplan bör innehålla tydliga målsättningar, ansvarsbeskrivningar för medverkande resurser, samt en konkret tidsram som arbetet för framtagning av ett ledningssystem ska förhålla sig till.
- Kommunen bör utreda möjligheten att upprätta en arbetsgrupp för informationssäkerhet som sammanträder regelbundet och inkluderar nyckelpersoner för arbetet. Denna grupp bör ha ansvar för förvaltning av ledningssystemet för informationssäkerhet och bör ha som uppgift att styra och samordna informationssäkerhetsarbetet inom hela kommunen. Arbetsgruppen bör vidare ha ett övergripande ansvar för omvärldsbevakning inom informationssäkerhetsområdet.
- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.
- Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Söderköpings kommun. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet
- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Kommunen bör genomföra systematiska uppföljningar av utbildningsverksamheten.
- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- Kommunen bör se över förvaltningsmodellen för verksamhetssystem och utreda möjligheter till att förstärka ansvaret som systemägare har för tillämpning av informationssäkerhetsåtgärder.

Bilaga 1

Dokumentationslista

Dokument	Diarienummer	Reviderad
Informationssäkerhetsinstruktion för användare i Söderköpings kommun 2018-2022	2018-00073	2019-07-26
Informationssäkerhetsinstruktion för drift och förvaltning i Söderköpings Kommun 2018-2022	2018-00073	2018-01-17
Informationssäkerhetsplan för Söderköpings kommun 2018-2022	2018-00073	2018-01-17
IT Plan för Söderköpings kommun 2018-2022	2018-00073	2018-03-27
Riktlinjer för chefer om kontroll av arbetstagares nyttjande av IT-utrustning och IT-resurser	2019-00303	2019-09-06

2022-01-25

Rebecka Hansson

Uppdragsledare