



Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Revisionens granskning av IT-säkerhet

Sammanfattning

På uppdrag av Trelleborgs kommuns förtroendevalda revisorer har EY genomfört en uppföljande granskning av kommunens arbete med informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende informationssäkerheten, samt följa upp på revisionsgranskningen genomförd 2019.

Baserat på den analys och granskning som genomförts bedöms Trelleborgs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en lite högre mognadsgrad, med ett genomsnitt på 2,77 jämfört med jämförelsetalet 2,39.

Kommunens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid, samt kontinuerlig utbildning inom informationssäkerhet och GDPR.

Iakttagelserna som noterades under granskningen av informationssäkerhet 2019 bedöms delvis åtgärdade av revisionen. Kommunledningsförvaltningen delar inte revisorernas uppfattning, då samtliga åtgärder förutom en är genomförda. Anledningen till att en av åtgärderna inte är tillfullo är hanterad beror på ett stundande systembyte, varför Kommunledningsförvaltningen inte bedömt att kostnaden för att genomföra förändringen kan motiveras ekonomiskt. Aktuellt nytt system införs 2022 och detta kommer att uppfylla de krav som ställs på program av denna dignitet. Kommunen har vidare bland annat upprättat centrala rutinbeskrivningar gällande programförändringar och IT-drift men saknar detaljerade rutinbeskrivningar för åtkomsthantering.

Beslutsunderlag

KS 2021/574 Tjänsteskrivelse Revisionens granskning av IT-säkerhet, 2021-09-02
Rapport: Informationssäkerhetsgranskning Juli 2021
Missiv IT säkerhet

Kommunledningsförvaltningens förslag till beslut

Kommunstyrelsens arbetsutskott föreslås besluta att föreslå Kommunstyrelsen besluta

att ge kommundirektören i uppdrag att ta fram rutiner för åtkomsthantering till kommunens verksamhetssystem

att ge kommundirektören i uppdrag att vartannat år se över policy för informationssäkerhet

att ge kommundirektören i uppdrag att varje år se över riktlinje för informationssäkerhet

Beslutet skickas till

Michel El-Dabh, enhetschef för Digital utveckling

Malin Ekblad Säkerhetschef

Ärendet

På uppdrag av Trelleborgs kommuns förtroendevalda revisorer har EY genomfört en uppföljande granskning av kommunens arbete med informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende informationssäkerheten, samt följa upp på revisionsgranskningen genomförd 2019.

Baserat på den analys och granskning som genomförts bedöms Trelleborgs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en lite högre mognadsgrad, med ett genomsnitt på 2,77 jämfört med jämförelsetalet 2,39.

Kommunens största förbättringsbehov består i att säkerställa att styrdokument och tillhörande riktlinjer gällande informationssäkerhet förblir aktuella över tid, samt kontinuerlig utbildning inom informationssäkerhet och GDPR.

Iakttagelserna som noterades under granskningen av informationssäkerhet 2019 bedöms delvis åtgärdade av revisionen. Kommunledningsförvaltningen delar inte revisorernas uppfattning, då samtliga åtgärder förutom en är genomförda. Anledningen till att en av åtgärderna inte är tillfullo är hanterad beror på ett stundande systembyte, varför Kommunledningsförvaltningen inte bedömt att kostnaden för att genomföra förändringen kan motiveras ekonomiskt. Aktuellt nytt system införs 2022 och detta kommer att uppfylla de krav som ställs på program av denna dignitet. Kommunen har vidare bland annat upprättat centrala rutinbeskrivningar gällande programförändringar och IT-drift men saknar detaljerade rutinbeskrivningar för åtkomsthantering.

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten utifrån revisionsgranskning genomförd 2019. Vidare är syftet också att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande frågor:

Har kommunen genomfört de rekommendationer som framkom i informationssäkerhetsgranskningen från 2019?

Iakttagelserna som noterades under granskningen av informationssäkerhet 2019 bedöms delvis åtgärdade. Kommunen har bland annat upprättat centrala rutinbeskrivningar gällande programförändringar och IT-drift men saknar detaljerade rutinbeskrivningar för åtkomsthantering. Sedan granskningen 2019 har en åtgärdsplan på 96 åtgärder tagits fram och samtliga punkter har enligt intervjuer med nyckelpersonen åtgärdats.

Har kommunstyrelsen vidtagit åtgärder för att göra regelverk kända i organisationen och ta fram detaljerade rutinbeskrivningar för områdena: åtkomst, änderingshantering och drift?

Kommunen har bland annat tagit fram rutinbeskrivningar över hur kommunens IT-avdelning arbetar med att registrera och behandla behov och önskemål om

förändringar, samt genomför och utvärderar förändringar, i kommunens IT-tjänster. Vidare har kommunstyrelsen tagit fram beskrivningar kring infrastrukturen och systemdrift för IT. Det saknas däremot detaljerade rutinbeskrivningar för åtkomsthantering.

Har kommunstyrelsen vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav?

Kommunstyrelsen bedöms ha vidtagit åtgärder för att säkerställa att stöd och resurser finns för att de olika förvaltningarna skall ha möjlighet att skapa ändamålsenliga rutiner för att uppfylla uppställda krav.

Har kommunstyrelsen tagit fram en handlingsplan för att prioritera arbetet utifrån angelägenhetsgrad?

En handlingsplan på 96 punkter uppdelat på de fyra systemen som granskningen 2019 omfattade togs fram efter granskningen. Handlingsplanen anger identifierad brist, ansvarig person och deadline för respektive åtgärd. Enligt intervjuade nyckelpersoner har samtliga 96 identifierade brister blivit åtgärdade. Revisorerna menar att då de saknas prioritering av arbetet mellan de olika åtgärderna, det saknas spårbarhet i handlingsplanen i form av status för åtgärderna samt att de utsatta deadlines för åtgärderna inte hållits anses denna revisionsfråga endast delvis uppfylld.