Kommunstyrelsen

2024-05-14
TJÄNSTESKRIVELSE
Dnr: KFKS-2024-00416

Revisionsskrivelse och revisionsrapport 2023:14 – Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår att kommunstyrelsen beslutar följande.

1. Kommunstyrelsen antar yttrande över revisionsrapport och revisionsskrivelse 2023:14 enligt bilaga 3 till tjänsteskrivelse daterad den 14 maj 2024.
2. Kommunstyrelsens beslut justeras i omedelbar anslutning till sammanträdet.

Sammanfattning av ärendet

Granskningen avser bedöma om kommunstyrelsen har säkerställt ändamålsenlig styrning, intern kontroll och uppföljning av hanteringen av de IT-system som är centrala för kommunens finansiella rapportering. Revisionens samlade bedömning är att kommunstyrelsen inte i tillräcklig utsträckning har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av behörigheter, programförändringar och IT-drift för de system som granskats.

Ärendet

Innehållet i revisionsgranskningen i korthet samt och revisorernas rekommendationer

EY har på uppdrag av de förtroendevalda revisorerna i Nacka kommun granskat behörighets-, programförändrings- samt IT-driftshantering inom tre av kommunens IT-system: ekonomisystemet UBW, lönesystemet Personec och försörjningsstödssystemet Lifecare.

Granskningen avser bedöma om kommunstyrelsen har säkerställt ändamålsenlig styrning, intern kontroll och uppföljning av hanteringen av de IT-system som är centrala för kommunens finansiella rapportering. Granskningens iakttagelser och bedömningar grundas på genomförda intervjuer med ansvariga för respektive system samt genomgång av mottagen dokumentation för de områden som berörs.

Revisionens samlade bedömning är att kommunstyrelsen inte i tillräcklig utsträckning har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av behörigheter, programförändringar och IT-drift för de system som granskats. Däremot finns i många fall informella rutiner som inte är dokumenterade. Bland annat saknas en formellt beslutad rutin för regelbunden genomgång av användare inom ett system, en formellt beslutad ansvarsfördelning avseende förändringshantering inom ett system och en dokumenterad processbeskrivning för hantering av misslyckade schemalagda körningar inom ett system. Avslutningsvis har kommunen inte säkerställt att beslutade krav avseende säkerhetsinställningar efterlevs, då ett systems lösenordskrav inte möter de krav som ställs enligt kommunens lösenordspolicy samt då kommunen för ett annat system inte kunnat visa att lösenordsinställningarna lever upp till kraven.

I granskningen har EY identifierat ett antal förbättringsområden och rekommenderar att kommunstyrelsen i Nacka kommun säkerställer att:

- Relevanta styrdokument och kontroller finns framtagna och att tillhörande riktlinjer dokumenteras och implementeras.
- Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.
- Roll- och ansvarsfördelningar förtydligas och beslutas

Stadsledningskontorets synpunkter samt förslag på yttrande

Relevanta styrdokument och kontroller finns framtagna och att tillhörande riktlinjer dokumenteras och implementeras

Stadsledningskontoret bedömer att det redan idag finns en tydlig dokumentation samt etablerade processer inom området. Denna dokumentation och processbeskrivning uppfyller merparten av det brister som revisionsrapporten pekar på. Av det underlag som revisorerna tagit del av, utifrån bland annat intervjuer, är det dock tydligt att processerna inte fullt ut är implementerade och kända av alla berörda medarbetare och chefer på verksamhetssidan. Revisionen visar på vikten av att både kommunens verksamheter och IT-funktion är insatta och involverade i arbetet med systemfrågorna, att verksamhet och IT arbetar tillsammans i högre utsträckning, samt att objektsförvaltningen är prioriterad och följs upp systematiskt av chefer. Stadsledningskontoret föreslår därför en större insats med utbildning i objektsstyrning för verksamheterna och säkerställande att alla berörda medarbetare och chefer på alla nivåer inom objektsförvaltningen blir insatta i processerna och dokumentationen. Vidare föreslås årliga utbildningsinsatser för kunskapsrepetition samt information till nya medarbetare när de anställs i dessa roller hos verksamheterna. Ansvaret för att ge utbildning till nyanställda på verksamhetssidan i objektsförvaltning föreslås ligga hos objektsägare (ansvariga direktörer) men där digitaliseringsenheten tillhandahåller utbildningen.

Vad gäller just kontroller kan stadsledningskontoret konstatera att det finns ett årshjul för objektförvaltning. I detta årshjul finns en årlig rutin för att genomföra aktuella kontroller av till exempel behörighetsstyrning och säkerhetsåtgärder. Stadsledningskontoret bedömer därför att det redan finns etablerade kontrollfunktioner i denna del.

Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs

Behörighetshantering

Styrningen bedöms, till skillnad mot vad revisorerna anger, vara tillfredställande eftersom det finns framtagna rutiner i årshjul där ansvar och roller är utpekade. En utökad uppföljning på årsbasis kan däremot behöva införas samt utbildning av berörda medarbetare. Vad gäller behörigheter och lösenord i ekonomisystemet UBW kan det fortsatt utvecklas utifrån genomförd informationsklassning och systemsäkerhetsanalys.

Programförändringar

Stadsledningskontoret bedömer att det finns framtagna processer och arbetssätt generellt vad gäller programförändringar i kommunen. Däremot kan en kompletterande översyn göras specifikt för system som granskas för att utvärdera om ytterligare åtgärder behöver vidtas.

It-driftsrutiner

Stadsledningskontoret konstaterar att det finns ett behov att förtydliga roller och ansvar mellan leverantör och kommunen vad gäller outsourcade system där leverantören har driftsansvaret.

Åtgärder gällande behörighetshantering, programförändring och IT-driftsrutiner

Berörda objekt behöver utifrån ovan utvecklingsområden omgående planera för detta arbete genom att komplettera sina objektsplaner med föreslagna åtgärder. Digitaliseringsenheten kommer bistå med att tillhandahålla utbildningar inom ovan områden för objektens medarbetare och chefer samt stöttning i arbetet.

Roll- och ansvarsfördelningar förtydligas och beslutas

Av framtagen ”Nacka systemförvaltningsmodell” framgår redan roller och ansvar. Däremot behövs utbildning om detta för en bättre implementering.

Ekonomiska konsekvenser

Förslaget till beslut medför inga ekonomiska konsekvenser.

Konsekvenser för barn

Föreslaget till beslut medför inga konsekvenser för barn.

Handlingar i ärendet

Tjänsteskrivelse daterad den 14 maj 2024

1. Revisionsskrivelse 2023:14
2. Revisionsrapport 2023:14 (denna bilaga publiceras inte på nacka.se eftersom den i vissa delar kan omfattas av sekretesskydd enligt offentlighets- och sekretesslagen)
3. Förslag på yttrande

Henrik Palmblad Wennergren
Digitaliseringsdirektör
Stadsledningskontoret

Christer Lindberg
Finans- och ekonomidirektör
Stadsledningskontoret

Elisabeth Carle
HR-direktör
Stadsledningskontoret

Veronica Grimheden Myhrström
Utbildnings- och arbetsmarknadsdirektör
Stadsledningskontoret

Brita Molavi Rösberg
Enhetschef
Digitaliseringsenheten

Anneli Sagnérius
Kommunjurist
Juridik- och kanslistaben