TRONDHEIM KOMMUNE
Trondheim kommunerevisjon

Kontrollutvalget

Vår saksbehandler	Vår ref.	Deres ref.	Dato
Børge Sundli	21/21084 oppgis ved alle henv.		07.03.2022

Uavhengig revisors attestasjonsuttalelse om etterlevelse i økonomiforvaltningen, Generelle IT-kontroller med særlig fokus på datasikkerhet og beredskapstiltak i Trondheim kommune

Vi har utført et attestasjonsoppdrag som skal gi moderat sikkerhet, i forbindelse med Trondheim kommunes etterlevelse av bestemmelser knyttet til IT-sikkerhet.

Problemstilling og delproblemstillinger:
Har Trondheim kommune tilfredsstillende internkontroll i og rundt IT-systemene som genererer regnskapstall?

- Har Trondheim kommunen tilfredsstillende tilgangsadministrasjon til IT-systemene?
- Er det tilfredsstillende endringshåndtering av IT-systemer i Trondheim kommune?
- Har Trondheim kommune tilfredsstillende datasikkerhet og beredskapstiltak?

Kriteriene har vært:

- Kommunen skal ha tilfredsstillende tildeling, endring og sletting av tilganger til IT-systemer
- Kommunen skal ha tilfredsstillende endringshåndtering for IT-systemer
- Kommunen bør ha identifisert og vurdert risikoen for kommunens IT-funksjon
- Kommunen bør ha iverksatt tiltak for å sikre IT-systemer og IT-utstyr
- Kommunen bør følge opp og evaluere risikostyringen for IT-området
- Kommunen bør ha etablert planer for å håndtere uønskede hendelser

Revisjonskriterier er utledet fra følgende kilder:

- Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet.
- KS 2021, brev til kommuner og fylkeskommuner "Datasikkerhets- og beredskapstiltak i kommunal sektor".
- ISO 27000-serien og ISO 31000.
- ISAE 3402-uttalelser.
- Lov om kommunal beredskapsplikt § 17.

Postadresse:
Trondheim kommune
Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 TRONDHEIM

Besøksadresse:
Søndre gate 10B

Telefon:
72546440

Telefaks:

Organisasjonsnummer:
NO 942 110 464

E-postadresse: revisjon.postmottak@trondheim.kommune.no
www.trondheim.kommune.no

22000009060
36142/22

Ledelsens ansvar for etterlevelse av bestemmelser og vedtak for økonomiforvaltningen
Kommunedirektøren er ansvarlig for å etablere administrative rutiner som sørger for at økonomiforvaltningen utøves i tråd med bestemmelser og vedtak, og at økonomiforvaltningen er gjenstand for betryggende kontroll.

Vår uavhengighet og kvalitetskontroll
Vi har utført oppdraget i samsvar med etiske retningslinjer for kommunerevisjonen, som inneholder uavhengighetskrav og andre krav basert på grunnleggende prinsipper om integritet, objektivitet, faglig kompetanse og tilbørlig aktsomhet, fortrolighet og profesjonell opptreden. I samsvar med internasjonal standard for kvalitetskontroll (ISQC 1 Kvalitetskontroll for revisjonsfirmaer som utfører revisjon og forenklet revisorkontroll av regnskaper samt andre attestasjonsoppdrag og beslektede tjenester) har Trondheim kommunerevisjon et tilstrekkelig kvalitetskontrollsystem, herunder dokumenterte retningslinjer og rutiner for etterlevelse av etiske krav, faglige standarder og krav i gjeldende lovgivning og annen regulering.

Våre oppgaver og plikter
Vår oppgave er å avgi en uttalelse om etterlevelse av bestemmelser og vedtak for økonomiforvaltningen på grunnlag av bevisene vi har hentet inn. Vi har utført vårt attestasjonsoppdrag med moderat sikkerhet i samsvar med kommunelovens regler og RSK 301 Forenklet etterlevelseskontroll med økonomiforvaltningen. Standarden krever at vi planlegger og gjennomfører oppdraget for å oppnå moderat sikkerhet for hvorvidt det foreligger vesentlige feil eller mangler ved etterlevelse av bestemmelser og vedtak i kommunens økonomiforvaltning på det området vi har foretatt forenklet etterlevelseskontroll.

Vi baserer oppgaven på en risiko- og vesentlighetsvurdering.

Utføring av et attestasjonsoppdrag som skal gi moderat sikkerhet i henhold til RSK 301, innebærer å utføre handlinger for å innhente bevis for at bestemmelser og vedtak for økonomiforvaltningen etterleves. Typen, tidspunktet for og omfanget av de valgte handlingene er gjenstand for revisors skjønn. Moderat sikkerhet har klart lavere sikkerhetsgrad enn betryggende sikkerhet, og vi gir derfor ikke uttrykk for samme nivå av sikkerhet som i en revisjonsberetning.

Vi mener at vi har innhentet tilstrekkelig og hensiktsmessig bevis som grunnlag for vår konklusjon.

Grunnlag for konklusjon
Vi viser til vårt brev til organisasjonsdirektøren av 14. februar 2022 og tilsvar av 24. februar 2022.

Konklusjon
Basert på de utførte handlingene og innhentede bevis er vi ikke blitt oppmerksomme på noe som gir oss grunn til å tro at Trondheim kommune ikke i det alt vesentlige har tilfredsstillende internkontroll i og rundt IT-systemene som genererer regnskapstall.

Vi vil trekke frem følgende områder som bør ha særlig fokus fremover:

- Utarbeiding av en egen ROS-analyse for IT-området for å sikre et helhetlig bilde av risikoen for IT-driften i Trondheim kommune
- En tilstrekkelig overordnet plan for IT-sikkerhet
- Etablering av en plan for gjennomføring av krise- og beredskapsøvelser for IT-området

22000099060

36142/22

Denne uttalelsen er utelukkende utarbeidet for å gi kontrollutvalget et bedre grunnlag for å ivareta sitt påse ansvar med økonomiforvaltningen og til Trondheim kommunes informasjon, og er ikke nødvendigvis egnet til andre formål.

Med hilsen

Per Olav Nilsen
revisjonsdirektør

Børge Sundli
revisor/CISA

Elektronisk dokumentert godkjenning uten underskrift

Vedlegg: Brev til organisasjonsdirektøren av 140222
Svar fra organisasjonsdirektøren av 240222
Signert uttalelse fra ledelsen av 010322

Kopimottaker: Postmottak Kontrollutvalget, Kontrollutvalgets sekretariat
Trude Kristin Kjeldstad, Organisasjonsdirektøren
Bjørn Jonny Villa, IT-tjenesten
Ola Eirik Klingen, Organisasjonsdirektøren

22000009060

36142/22