Trondheim kommunerevisjon

Untatt offentlighet, jf offentlighetsloven §5-2

Rapport 3/2026-RE
Etterlevelseskontroll IT - Gat turnussystem

Forord

Trondheim kommunerevisjon har i denne etterlevelseskontrollen undersøkt om kommunen har definert ansvar og oppgaver mellom tjenesteforvalter, tjenesteeiere og bydelsområdene for IT-systemet Gat samt roller og tilganger til IT-systemet. Arbeidet med rapporten har foregått fra 19. juni 2025 til 24. april 2026. Byrådet har hatt rapporten til verifisering og uttalelse mellom 24. april 2026 og 1. juni 2026.

Arbeidet er utført av Elin Haarsaker (prosjektleder), Anne-Margit Eide Schjølberg og Aase Birgitte Nerland.

Dette er en forenklet etterlevelseskontroll med økonomiforvaltningen. Kontrollen skal skje i forlengelsen av revisjonen av regnskapet og skal rette seg mot de delene av økonomiforvaltningen som går ut over å uttale seg om årsregnskapet.

Kommunelovens § 24-9 forutsetter at revisor gir en egen uttalelse om kontrollen som er utført. Kontrollen skal gjennomføres med såkalt moderat sikkerhet. Kravene til denne kontrollen er definert gjennom god kommunal revisjonsskikk og revisjonsstandarden RSK 301 "Forenklet etterlevelseskontroll med økonomiforvaltningen".

Formelt består etterlevelseskontroller av tre deler. Disse tre delene er samlet sammen i denne rapporten. Den første delen er kommunerevisjonens brev til byrådet om etterlevelseskontrollen (kapittel 1 til og med kapittel 5). Den andre delen er svaret fra byrådet (kapittel 6 Byrådets uttalelse). Til sist formaliseres etterlevelseskontrollen gjennom en uttalelse fra revisor til kontrollutvalget. Revisors uttalelse ligger først i rapporten.

Trondheim, 2. juni 2026

Per Olav Nilsen

revisjonsdirektør

Elin Haarsaker

statsautorisert revisor

Uavhengig revisors attestasjonsuttalelse om etterlevelseskontroll IT - Gat turnussystem

Vi har utført et attestasjonsoppdrag som skal gi moderat sikkerhet for at Trondheim kommune har etablert tilfredsstillende styring og kontroll med roller og tilganger i Gat turnussystem.

Problemstillinger

Har Trondheim kommune god kontroll og oppfølging av turnussystemet Gat?

Vi har tre underproblemstillinger:

- Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?
- Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk[1]?
- Har kommunen sikret opplæring og støtte til de som bruker Gat?

Revisjonskriterier

Til de tre underproblemstillingene har vi følgende revisjonskriterier:

1. Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?
    - Kommunen skal ha skriftlige rutiner som beskriver fordeling av ansvar og hva som inngår i funksjonene til tjenesteforvalter, tjenesteeier, byrådsavdelinger og Trondheim digital.
    - Kommunen skal ha skriftlige retningslinjer som definerer hvordan tjenesteforvalter skal utøve sitt ansvar for roller og tilganger.

2. Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemet er i samsvar med tjenstlig behov[2] og gjeldende regelverk[3]?
    - Roller i Gat skal være satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
    - Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium, brukere skal kun ha tilgang til de rollene de trenger for å utføre sine arbeidsoppgaver.
    - Kommunen skal ha skriftlige rutiner for tildeling, endring og sletting/parkering av tilganger.
    - Kommunen skal jevnlig evaluere tilganger til roller i Gat for å sikre at ansattes rettigheter i systemet ivaretar ansattes behov ved utførelse av sine arbeidsoppgaver.

[1] Grunnprinsipper NSM, rutiner i Kvaliteket og GDPR. GDPR (General Data Protection Regulation) er EUs personvernforordning.

[2] Tjenstlig behov: Få rettigheter i systemet som er nødvendig for å kunne utføre sine arbeidsoppgaver.

[3] Grunnprinsipper NSM, rutiner i Kvaliteket og GDPR

- Loggføring av bruk av Gat skal gjennomgås jevnlig for å avdekke eventuelt misbruk.

3. Har kommunen sikret opplæring og støtte til de som bruker Gat?
    - Kommunen skal sikre opplæring og støtte til de som bruker Gat.
    - Kommunen bør sørge for opplæring av tjenesteforvalter i informasjonssikkerhet og personvern.

Revisjonskriteriene er utledet i kapittel 2, 3 og 4 fra følgende kilder:

- Kapittel 25. Internkontroll i kommuneloven
- NSM Grunnprinsipper for IKT-sikkerhet
- NSM - Sikkerhetsfaglig anbefalinger ved bruk av tjenesteutsetting og skytjenester
- KS brev til kommunene "Brev til kommunens IT-ansvarlig/IT-sikkerhetsansvarlig".
- Kjøreregler for bruk av informasjons- og kommunikasjonsteknologi (IKT) (4.1.23)
- Hovedrapport "Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune"
- 1.12.2022, unntatt offentlighet jfr. Offentlighetsloven § 24 tredje ledd.
- Personopplysningsloven (GDPR)[4]
- Trondheim Digital, rutine tjenesteforvalter Gat
- Kvaliteket[5]
    - 8884-1, Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune
    - 6006-7, IT-tilganger i Trondheim kommune
    - 4522-1, Retningslinjer for databehandleravtaler
    - 8882-2, Retningslinje for sikkerhetsrevisjon og testing av IT-systemer
    - 8883-2, Retningslinje - krav til autentisering for tilgang til tjenester i Trondheim kommune
    - 4493-1, Tjenestestyring av IT løsninger i Trondheim kommune
    - 6014-1, Tjenesteforvalter av IT-løsninger av IT-løsninger

Ledelsens ansvar for etterlevelse av bestemmelser og vedtak for økonomiforvaltningen

Byrådet 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 (ISQM 1 Kvalitetskontroll for revisjonsfirmaer som utfører revisjon og forenklet revisorkontroll av regnskaper samt andre

[4] Lov om behandling av personopplysninger (personopplysningsloven).

[5] Kvaliteket er kommunens kvalitetssystem og inneholder kommunens rutiner og dokumenter på ulike områder. Det er et IT-basert verktøy som er tilgjengelig for alle ansatte.

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 byråd for finans 19. mai 2026 og tilsvar 1.juni 2026. Nedenfor gjengis revisjonens anbefalinger i brevet med svarene fra administrasjonen:

Har Trondheim kommune god kontroll og oppfølging av turnussystemet Gat?

Vi har tre underproblemstillinger:

- Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?
- Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk[6]?
- Har kommunen sikret opplæring og støtte til de som bruker Gat?

Revisjonens undersøkelser viser at kommunen ikke har hatt tilfredsstillende kontroll og oppfølging av turnussystemet Gat spesielt knyttet til definering av ansvar og styring av roller og tilganger.

Konklusjon med forbehold

Basert på de utførte handlingene, innhentede bevis og byrådets svar, kan vi ikke konkludere med at kommunen har hatt tilfredsstillende kontroll og oppfølging av turnussystemet Gat spesielt

[6] Grunnprinsipper NSM (Nasjonal sikkerhetsmyndighet), rutiner i Kvaliteket og GDPR. GDPR (General Data Protection Regulation) er EUs personvernforordning.

knyttet til definering av ansvar og styring av roller og tilganger. Byråden for finans har i sin høringsuttalelse gitt tilbakemelding på funnene i vår undersøkelse. Se punkt 6 i rapporten.

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.

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Trondheim kommunerevisjon har de siste årene gjennomført årlige etterlevelseskontroller av kommunens IT-område. Vår kontakt med tjenesteforvaltere i disse kontrollene og "Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune" fra 2022 tyder på at ansvar og oppgaver for ulike IT-systemer ikke er godt nok beskrevet eller avklart.

Risiko- og sårbarhetsanalysen fra 2022 viste at mange av svakhetene lå hos de enkelte virksomhetsområdene,[7] og ikke hos Trondheim Digital.[8] Dette knyttet seg særlig til rollen som tjenesteforvalter og mangelfulle rutiner for denne funksjonen. I etterlevelseskontrollen fra 2023[9] konkluderte vi med at kommunen manglet retningslinjer for hvordan tjenesteforvalter, tjenesteeiere og virksomhetsområder skulle følge opp tilgangsrettigheter.

Etterlevelseskontrollen fra 2024[10] viste at det manglet skriftlige rutiner for å opprette, endre, slette og evaluere roller i IT-systemene i kommunen. Skriftlige rutiner er viktige for å sikre riktige tilganger og god sikkerhet. Tilgangene til tre av fem systemer som inngikk i undersøkelsen, var ikke satt opp etter prinsippene om minst mulig privilegium.

I år har vi valgt å kontrollere IT-systemet Gat. Systemet brukes ved flere byrådsområder[11], generer variabel lønn for turnusbaserte tjenester og har derfor betydning for kommunens økonomi. I 2025 utgjorde lønnsutgifter fra Gat over 400 millioner kroner. Kommunen har cirka 18 000 brukere av Gat. Det er derfor viktig at brukere har fått tilstrekkelig opplæring i bruk av Gat og det er viktig at kommunen har kontroll på innholdet i rollene og tildeling av roller i Gat. I Gat brukes begrepet brukergruppe om roller, men vi bruker begrepet rolle i denne rapporten for å være systemuavhengig. Gat har ifølge tjenesteforvalter vært i bruk i kommunen siden rundt 2002.

1.2 Definisjoner

Tjenesteforvalter
En tjenesteforvalter i Trondheim kommune er en person som har fagkompetanse knyttet til tjenesteområdet og som har ansvar for den daglige forvaltningen av hele eller deler av et IT-system, herunder å administrere tilganger til IT-systemet. Tjenesteforvalter er et bindeledd på operativt nivå mellom leverandøren og kommunen. Manglende føringer for rollen som tjenesteforvalter kan medføre at det blir opp til den enkelte tjenesteforvalter å definere og utøve sitt ansvar.

[7] Trondheim kommune var frem til innføring av parlamentarisme delt inn i sju virksomhetsområder: Byutvikling, Finans, Helse og velferd, Kultur, idrett og friluftsliv, Miljø, næring og samferdsel, Oppvekst og utdanning og Organisasjon.

[8] Trondheim Digital er kommunen sin IT-tjeneste.

[9] "Roller og ansvar til tjenesteforvalter, tjenesteeier, virksomhetsområdet og IT-tjenesten".

[10] "Roller og tilganger til fem utvalgte IT-systemer".

[11] Byrådsområder: Byutvikling, Finans, Helse og omsorg, Kultur, idrett og friluftsliv, Miljø, næring og samferdsel, Oppvekst og utdanning, Sosiale tjenester og byrådsleders avdeling.

Tjenesteeier
En tjenesteeier er systemeier for IT-system. Dette er ofte en enhet i Trondheim kommune.

Administrator
En administrator i GAT er en person med utvidede tilganger og ansvar for å konfigurere, drifte og vedlikeholde systemet.

Rolle
En rolle i IT-systemer gir den ansatte rettigheter til å se data eller utføre oppgaver i det aktuelle IT-systemet. Roller i IT-systemer definerer hvilke rettigheter brukere får i systemet. Ved implementering av nye IT-systemer er det vanligvis opprettet roller fra leverandørene.

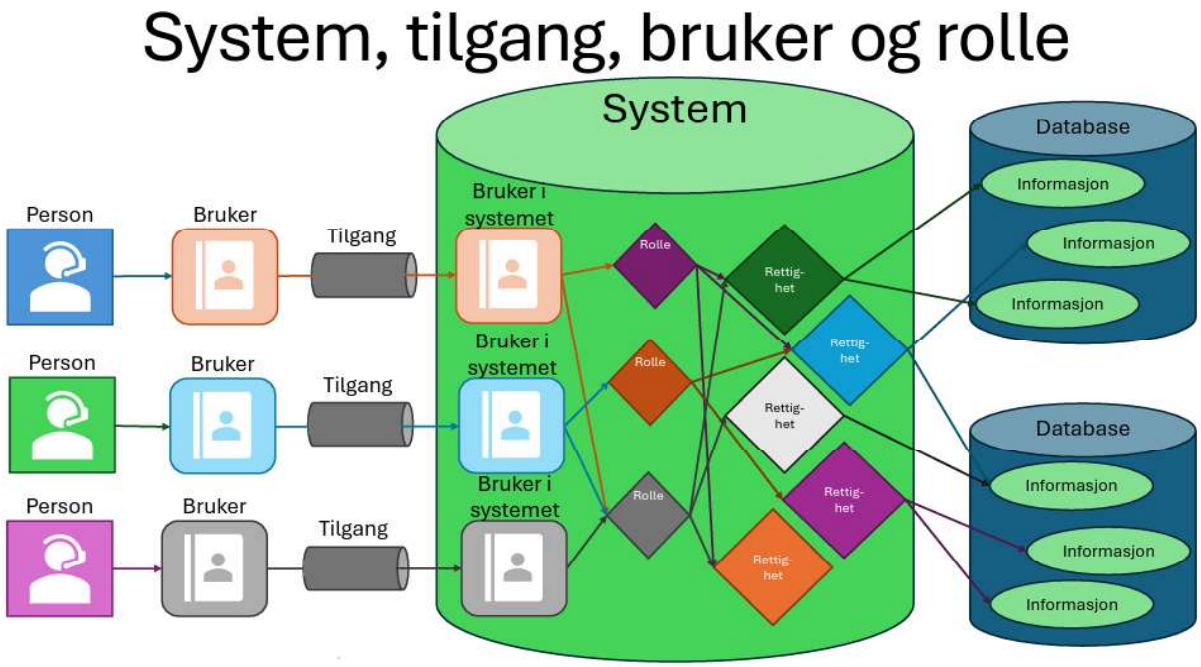
Bruker
Bruker er den identiteten den ansatte får i TK-nettet.

Autorisert bestiller
Person (ofte en enhetsleder) med fullmakt til å bestille tilgang til IT-systemer for sine ansatte.

Kvaliteket
Er kommunens kvalitetssystem og inneholder kommunens rutiner og dokumenter på ulike områder. Det er et IT-basert verktøy som er tilgjengelig for alle ansatte.

En ident
En ident (identitet) i et IT-system er et unikt digitalt sett med data som representerer en bruker, en enhet (som en PC eller mobil) eller en applikasjon. Denne identiteten brukes til å gjenkjenne, verifisere (autentisere) og gi tilgang (autorisere) til ressurser i et digitalt miljø.

Figur 1: Beskrivelse av system, tilgang, bruker og rolle



Forklaring på figur:

En nyansatt i kommunen får opprettet en bruker i kommunes intranett (TK-nett). Basert på informasjon fra autorisert bestiller oppretter IT-brukerhjelp en tilgang i det aktuelle IT-systemet. Den ansatte får da opprettet en bruker i systemet. For at man skal kunne se data eller utføre noe i systemet, må tjenesteforvalter legge til en eller flere roller til den ansattes bruker. Det er rollene som gir den ansatte rettigheter til å se data eller utføre oppgaver i IT-systemet. Alle data og informasjon i systemet ligger lagret i databaser. Tildelte roller gir brukeren tilgang til rettighetene de skal ha for å kunne utføre sin jobb i kommunen. Rollene i IT-systemer skal settes opp i henhold til kommunens behov og sikre at ansatte kun får tilgang til den informasjonen og de funksjonene de trenger for å utføre jobben sin. Roller skal være utformet slik at de sikrer at kommunen overholder lover og regler for informasjonssikkerhet og personvern. Det er derfor viktig å ha rutiner for håndtering og jevnlig evaluering av roller.

1.3 Problemstilling og avgrensning

Forenklet etterlevelseskontroll gjelder kontroll av økonomiforvaltningen. Undersøkelsen begrenses derfor til IT-systemer som behandler transaksjoner som inngår i kommunens regnskap.

Vi har følgende hovedproblemstilling:

Har Trondheim kommune god kontroll og oppfølging av turnussystemet Gat?

Vi har tre underproblemstillinger:

- Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?
- Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk[12]?
- Har kommunen sikret opplæring og støtte til de som bruker Gat?

1.4 Metode

Metodisk baserer undersøkelsen seg på:

- revisjonens kjennskap til systemet fra tidligere års revisjoner
- spørreundersøkelse
- intervju.

Vi har avgrenset undersøkelsen til ledernivå: kommunaldirektører, kommunalsjefer og enhetsledere og tjenesteforvalter for Gat.

[12] Grunnprinsipper NSM (Nasjonal sikkerhetsmyndighet), rutiner i Kvaliteket og GDPR. GDPR (General Data Protection Regulation) er EUs personvernforordning.

Intervju
Vi har intervjuet:

- tjenesteforvalter for Gat
- merkantile ved en enhet

Basert på svar i spørreundersøkelsen har vi hatt oppfølgingssamtaler med:

- enhetsleder ved et BoA
- enhetsleder ved et helse- og velferdssenter.

Spørreundersøkelse
Vi har gjennomført en spørreundersøkelse til 24 ledere som bruker Gat ved sine enheter, herunder to kommunaldirektører, seks kommunalsjefer og 16 enhetsledere. Vi har fått svar fra alle de 24 som er forespurt.

1.5 Revisjonskriterier

Til de tre underproblemstillingene har vi følgende revisjonskriterier:

4. Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?
    - Kommunen skal ha skriftlige rutiner som beskriver fordeling av ansvar og hva som inngår i funksjonene til tjenesteforvalter, tjenesteeier, byrådsavdelinger og Trondheim digital.
    - Kommunen skal ha skriftlige retningslinjer som definerer hvordan tjenesteforvalter skal utøve sitt ansvar for roller og tilganger.

5. Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemet er i samsvar med tjenstlig behov[13] og gjeldende regelverk[14]?
    - Roller i Gat skal være satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
    - Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium, brukere skal kun ha tilgang til de rollene de trenger for å utføre sine arbeidsoppgaver.
    - Kommunen skal ha skriftlige rutiner for tildeling, endring og sletting/parkering av tilganger.
    - Kommunen skal jevnlig evaluere tilganger til roller i Gat for å sikre at ansattes rettigheter i systemet ivaretar ansattes behov for å utføre sine arbeidsoppgaver.
    - Loggføring av bruk av Gat skal gjennomgås jevnlig for å avdekke eventuelt misbruk.

6. Har kommunen sikret opplæring og støtte til de som bruker Gat?
    - Kommunen skal sikre opplæring og støtte til de som bruker Gat.
    - Kommunen bør sørge for opplæring av tjenesteforvalter i informasjonssikkerhet og personvern.

[13] Tjenstlig behov: Rettigheter i systemet som er nødvendig for å kunne utføre sine arbeidsoppgaver.

[14] Grunnprinsipper NSM, rutiner i Kvaliteket og GDPR

Revisjonskriteriene er utledet i kapittel 2, 3 og 4 og fra følgende kilder:

- Kommuneloven kapittel 25 Internkontroll
- NSM Grunnprinsipper for IKT-sikkerhet
- NSM - Sikkerhetsfaglig anbefalinger ved bruk av tjenesteutsetting og skytjenester
- KS's "Brev til kommunens IT-ansvarlig/IT-sikkerhetsansvarlig".
- Kjøreregler for bruk av informasjons- og kommunikasjonsteknologi (IKT) (4.1.23)
- Hovedrapport "Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune" - 1.12.2022, unntatt offentlighet jfr Offentlighetsloven § 24 tredje ledd.
- Personopplysningsloven (GDPR)[15]
- Trondheim Digital, rutine tjenesteforvalter Gat
- Kvaliteket
    - 8884-1, Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune
    - 6006-7, IT-tilganger i Trondheim kommune
    - 4522-1, Retningslinjer for databehandleravtaler
    - 8882-2, Retningslinje for sikkerhetsrevisjon og testing av IT-systemer
    - 8883-2, Retningslinje - krav til autentisering for tilgang til tjenester i Trondheim kommune
    - 4493-1, Tjenestestyring av IT løsninger i Trondheim kommune
    - 6014-1, Tjenesteforvalter av IT-løsninger av IT-løsninger

[15] Lov om behandling av personopplysninger (personopplysningsloven).

2 Rutiner for fordeling av ansvar for IT-systemet Gat

2.1 Revisjonskriterier

- Kommunen skal ha skriftlige rutiner som beskriver fordeling av ansvar og hva som inngår i funksjonene til tjenesteforvalter, tjenesteeier, byrådsavdelinger og Trondheim digital.
- Kommunen skal ha skriftlige retningslinjer som definerer hvordan tjenesteforvalter skal utøve sitt ansvar for roller og tilganger.

2.2 Skriftlige rutiner for fordeling av ansvar

Trondheim kommune har valgt å fordele ansvar knyttet til IT-systemer mellom fire ansvarsnivåer. Disse er tjenesteforvalter, tjenesteeier, byrådsområdet og Trondheim Digital (tidligere IT-tjenesten). Revisjonen har i spørreundersøkelsen spurt om kommunen har skriftlige rutiner og retningslinjer for fordeling av ansvar ved behov for nye roller eller endringer i eksisterende roller i Gat mellom de fire ansvarsområdene. Svarene fra de 24 forespurte fordeler seg slik:

Tabell 1: Antall svar på spørsmål om kommunen har skriftlige rutiner og retningslinjer for fordeling av ansvar ved behov for nye roller eller endringer i eksisterende roller i Gat

	Ja	Nei	Vet ikke
mellom byrådsområdet/enheten og tjenesteeier	7	1	16
mellom byrådsområdet/enheten og tjenesteforvalter	6	1	17
mellom byrådsområdet/enheten og Trondheim Digital	6	1	17

Sju av 24 personer har svart at de har skriftlige rutiner for fordeling av ansvar mellom byrådsområdet/enheten og tjenesteeier. Fire av de sju viser til Kvaliteket og til rutiner for tildeling av tilgang til IT-systemer. Ingen av disse sju personene viser til konkrete skriftlige rutiner for fordeling av ansvar ved behov for nye roller eller endring av eksisterende roller i Gat.

Seks av 24 personer har svart at de har skriftlige rutiner for fordeling av ansvar mellom byrådsområdet/enheten og tjenesteforvalter. Ingen av de seks personene viser til konkrete skriftlige rutiner for fordeling av ansvar ved behov for nye roller eller endring av eksisterende roller i Gat. Fire personer viser til Kvaliteket og til rutiner for tildeling av tilgang til IT-systemer.

Seks av 24 personer har svart at de har skriftlige rutiner for fordeling av ansvar mellom byrådsområdet/enheten og Trondheim Digital. Ingen av de seks personene viser til konkrete skriftlige rutiner for fordeling av ansvar ved behov for nye roller eller endring av eksisterende roller i Gat.

I vår etterlevelseskontroll fra 2024[16] anbefalte vi at byrådet burde etablere skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen. Dette var for å sikre at rollene er satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet. Oppfølging av denne etterlevelseskontrollen er fortsatt under arbeid.

Revisjonens vurderinger

Undersøkelsen viser at de fleste lederne ikke vet om det finnes skriftlige rutiner og retningslinjer for fordeling av ansvar mellom de fire ansvarsnivåene ved behov for nye roller eller endringer i eksisterende roller i Gat. Slik vi gjorde i etterlevelseskontrollen i 2024 anbefaler vi på nytt at det etableres skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen. Disse rutinene/retningslinjene bør beskrive ansvarsfordelingen for innholdet i rollene i Gat mellom de fire ansvarsnivåene.

2.3 Skriftlige retningslinjer for tjenesteforvalter sitt ansvar

Trondheim kommune har etablert en rutine for tjenesteforvalter for Gat.[17] Denne rutinen ligger ikke i Kvaliteket, men i Trondheim kommune sitt intranett under Trondheim Digital. Rutinen beskriver: strategi, operativ drift, nye behov, endringshåndtering, dokumentasjon, tilgangshåndtering, support, kurs og opplæring, personvern, samhandling, avtale og økonomi. Rutinen beskriver imidlertid ikke hvordan roller løpende skal vurderes i Gat.

Revisjonens vurderinger

Trondheim kommune har etablert en rutine for tjenesteforvalter for Gat. Rutinen fremstår som detaljert og godt beskrevet for daglig drift, men det mangler beskrivelse av hvordan roller løpende skal vurderes i Gat. Etter revisjonens vurdering bør det framgå av rutinen hvem som skal beslutte endringer i innhold og rettigheter i de ulike rollene og om det eventuelt bør opprettes nye roller ved endrede behov.

[16] "Rapport 7/2025-RE Etterlevelseskontroll IT-roller og tilganger for utvalgte systemer".

[17] Rutine tjenesteforvalter Gat

3 Kontroll med roller og tilganger til GAT

3.1 Revisjonskriterier

- Roller i Gat skal være satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
- Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium, brukere skal kun ha tilgang til de rollene de trenger for å utføre sine arbeidsoppgaver.
- Kommunen skal ha skriftlige rutiner for tildeling, endring og sletting/parkering av tilganger.
- Kommunen skal jevnlig evaluere ansattes tilgang til roller i Gat for å sikre at rettighetene i systemet samsvarer med det de ansatte trenger for å gjøre sine arbeidsoppgaver.
- Loggføring av bruk av Gat skal gjennomgås jevnlig for å avdekke eventuelt misbruk.

3.2 Roller i Gat er i samsvar med kommunens behov og betryggende sikkerhet

Roller som gis automatisk på grunnlag av stilling i kommunen
Rollene "MinGat", "Enhetsleder" og "Avdelingsleder" i Gat gis automatisk på grunnlag av sin stilling i kommunen.

Alle ansatte i Trondheim kommune får tilgang til Gat og blir tildelt rollen "MinGat" ved ansettelse. I hovedsak er det ansatte i enheter som har turnusbaserte tjenester som benytter MinGat.

Enhetsledere og avdelingsledere får automatisk tildelt rollene "Enhetsleder" og "Avdelingsleder" i Gat. Lederne gis full registreringstilgang til egen enhet og både enhetsleder og avdelingsleder kan anvise timelistene i Gat.[18] Avdelingsleder kan også attestere[19] timelister, men det er satt på sperre for at samme leder både kan attestere og anvise på samme timeliste.

Roller som må bestilles
Utvidede roller (roller med større rettigheter) i GAT bestilles på Trondheim kommune sin intranettside. Dette er roller til ansatte som ikke er ledere: "Bruker 1", "Merkantil" og "Vaktansvarlig".

På intranettsiden er det en overordnet, men ikke detaljert beskrivelse av hvilke rettigheter som inngår i rollene. Det er kun autoriserte bestillere som har tilgang til å bestille utvidede roller og som kan se beskrivelsene av innholdet i disse rollene. Revisjonen har i møter fått opplyst fra noen enhetsledere og merkantile at det er uklart for dem hvilke rettigheter som ligger i de ulike rollene i Gat. Det er derfor usikkerhet knyttet til hvilke roller de ansatte skal ha. Vi beskriver her rettigheter som ligger i de utvidede rollene:[20]

[18] Timelistene i Gat har tre signeringsnivå, ansatt, attestant og anviser. Ved anvisning av timelister signerer lederen på at timene kan utbetales.

[19] Attestere betyr å godkjenne at timene er korrekte og gyldige i henhold til retningslinjer for internkontroll.

[20] Vi beskriver ikke alle rettighetene, kun de viktigste forskjellene i de ulike rollene. Disse rollene krever tilgang til Citrix, som eventuelt må bestilles i tillegg. Enhetene må betale for Citrix-lisensene. Citrix er en programvareplattform som lar brukere få sikker, ekstern tilgang til Gat fra hvilken som helst enhet.

Rollen “Bruker1” har full registreringstilgang til egen enheten, men kan ikke godkjenne timelister og har ikke tilgang til Gat analyse[21]. For øvrig har denne rollen tilnærmet samme rettigheter som rollene “Enhetsleder” og "Avdelingsleder". Revisjonen har tidligere sett at rollen “Bruker1” har blitt misbrukt av en ansatt ved å legge inn bytte av vakter på seg selv uten å slette de opprinnelige vaktene. Det medførte at vedkommende fikk betalt lønn både for de opprinnelige vaktene, som vedkommende hadde byttet bort og ikke hadde jobbet, og de nye vaktene.

Rollen “Merkantil” har utvidede rettigheter i Gat og kan blant annet registrere endringer i vaktboken, godkjenne vaktbytter og overtid, attestere på timelistene og overføre godkjente timer til lønnsutbetaling. Merkantil skal blant annet kontrollere at timene blir riktig bokført og knyttet til riktig stilling i lønnssystemet. Merkantil attesterer for denne kontrollen, men har ofte ikke god nok forutsetning for å bekrefte at timelønnen er gyldig. Merkantile kan også signere for ansatte i Gat dersom ansatte ikke har signert sine timer selv.

Roller som både kan delegeres og bestilles
Rollen “Vaktansvarlig” og rollen “MinGatLeder”[22] kan både delegeres og bestilles. Enheten kan selv gi tilgang til disse to rollene. En ansatt som allerede er vaktansvarlig (har rollen Vaktansvarlig), kan tildele (delegere) denne rollen til andre ved enheten. De to enhetslederne vi intervjuet var ukjent med at dette var mulig. De er ikke enige i denne delegeringen fordi de som enhetsleder kan miste kontroll over hvem som har rollen.

Dersom en ansatt har behov for tilgang til andre enheter enn egen enhet, må en autorisert bestiller bestille tilgangen. Rollen “Vaktansvarlig” kan registrere og godkjenne endringer i vaktboken i Gat. Ansatte med rollen “MinGatLeder” (web-klient)[23] kan ikke godkjenne endringer (for eksempel ekstra innleie av personell, bytter av vakter og overtid) i Gat.

Godkjenning av timelister
Timelistene i Gat har tre signeringsnivåer: ansatt, attestant og anviser. Ansatte signerer sine egne timelister i MinGat. Rollen "Merkantil" attesterer timelister og rollen "Enhetsleder" anviser timelister. Når timelistene attesteres av "Merkantil", innebærer dette en godkjenning av at bokføringen riktig, men ikke at selve timene er gyldige.

Kjennskap til rollene “Bruker1” og “ Vaktansvarlig”
I spørreundersøkelsen spurte vi lederne om de kjente til hvilke rettigheter som ligger i rollene “Bruker1” og “Vaktansvarlig”. Revisjonen valgte ut disse to rollene på grunn av risiko knyttet til utvidede rettigheter og det høye antallet brukere som har disse rollene. Spørsmålene ble bare sendt til enhetslederne, ikke til kommunalsjef og kommunaldirektør.

[21] I Gat Analyse kan en blant annet overvåke kostnadsutviklingen og analysere fraværet.

[22] “MinGatleder” benyttes kun i web-versjonen av Gat. Citrixløsning er ikke nødvendig. Rollen var ment som en erstatning for rollen “Vaktansvarlig” i Citrixløsningen.

[23] Gat web-klient (ofte referert til som MinGat eller Ressursstyring WEB) er en nettleserbasert løsning for Visma Gat ressursstyringssystem. Det er en selvbetjeningsportal der ansatte som jobber i turnus eller med beredskap kan administrere sin egen arbeidshverdag

Tabell 2: Antall enhetsledere som svarer at de kjenner til hvilke rettigheter som ligger i rollene "Bruker1" og "Vaktansvarlig"

Spørsmål	Ja	Nei	Vet ikke
Kjenner du til hvilke rettigheter som ligger i rollen "Bruker1"?	10	4	2
Kjenner du til hvilke rettigheter som ligger i rollen "Vaktansvarlig"?	12	3	1

De fleste enhetslederne, henholdsvis 10 og 12, svarte at de kjenner hvilke rettigheter som ligger i disse to rollene.

Tjenesteforvalter har imidlertid opplyst at det ikke finnes noen beskrivelser av hva som er rettighetene i de ulike rollene i Gat. Det er kun adminstratorer som kan se den detaljerte oversikten over hvilke rettigheter som inngår i de ulike rollene i Gat .

Revisjonens vurderinger

Revisjonen mener det er uheldig at det ikke finnes en lett tilgjengelig beskrivelse av hvilke rettigheter som inngår i de ulike rollene i Gat. En slik beskrivelse er nødvendig for å sikre at enhetene er i stand til å bestille de riktige rollene som gjør de ansatte i stand til å utføre sine arbeidsoppgaver. Ansatte skal ikke ha større rettigheter i Gat enn det de trenger for å utføre sine arbeidsoppgaver. En beskrivelse av rettigheten i rollene kan bidra til å redusere risikoen for at ansatte får tilgang til rettigheter utover tjenstlig behov. Rettigheter utover tjenstlig behov kan medføre økt risiko for misbruk av roller og risiko for bevisste og ubevisste feil.

Revisjonen anbefaler at det utarbeides eller gjøres tilgjengelig en beskrivelse av hvilke rettigheter som inngår i de ulike rollene i Gat. Det vil gjøre det enklere for lederne å bestille de rollene i Gat som de ansatte trenger for å utføre sine arbeidsoppgaver.

Revisjonen mener det er positivt at timelistene i Gat har tre signeringsnivå og at det er satt sperre for at samme person ikke både kan attestere og anvise på samme timeliste.

Revisjonen mener det er en risiko at det er rollen "Merkantil" som kan attestere timelister. Den som attesterer skal bekrefte at de registrerte timene i Gat stemmer med utført arbeid. Vi vurderer at merkantilt personale i mange tilfeller kan ha for lite kjennskap til timene for å kunne attestere. Som eksempel kan nevnes at merkantile for BoA er samlokalisert og har ikke fysisk arbeidsted på BoA.

Revisjonen anbefaler at byrådet vurderer om dagens roller i Gat dekker enhetenes behov uten at ansatte får for omfattende rettigheter i systemet. Mange ansatte i kommunen har rollene "Bruker1" og "Vaktansvarlig" som begge gir utvidede tilganger. Byrådet bør vurdere om rollene i Gat kan justeres, eller om det bør opprettes nye roller i systemet. Dette er nødvendig for å sikre at rollene er i samsvarer med kommunens behov og ivaretar betryggende sikkerhet.

3.3 Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium

Tilganger til Gat gis i web-versjon eller via en Citrix-løsning[24]. Alle ansatte i kommunen får automatisk tilgang til web-versjonen med rollen "Min Gat".[25] Det er to versjoner av systemet Gat, med ulike typer tilganger og roller. Siden Citrix-lisenser medfører store kostnader, besluttet Trondheim digital å slette disse lisensene for ansatte med vaktansvarlig-rollen. Som erstatning ble den nye rollen "MinGatLeder" opprettet i webversjonen. Rollen "Vaktansvarlig" ble imidlertid ikke slettet fra brukerne som mistet Citrix-lisensene.

Rollen "MinGatLeder" i web-versjonen har mer begrensede rettigheter enn vaktansvarlig-rollen i Citrix-versjonen. Rollen "MinGatLeder" kan ikke godkjenne endringer i Gat (eksempelvis ekstra innleie av personell, bytter av vakter og overtid). Rollen "Vaktansvarlig" kan imidlertid både registrere og godkjenne denne typen endringer i vaktboken i Gat. Dersom enhetene ønsker at ansatte fortsatt kan bruke vaktansvarlig-rollen, må de selv betale for Citrix-lisensene. Det er ikke tilsvarende kostnad for web-versjonen.

Det finnes ingen oversikt i Gat som viser hvem som har aktive "Vaktansvarlig-roller". I utgangspunktet gis rettigheter i Gat via tildeling av roller til ansatte. Vi har observert at det er mulig å gi enkeltrettigheter direkte til en ansatt ut over de rettighetene som ligger i deres tildelte roller i Gat. Det er administratorer som har mulighet for å gi ansatte slike tilleggsrettigheter. Tjenesteforvalter har tatt ut en rapport som viser hvilke tilleggsrettigheter som er gitt til ansatte, men enhetene har ikke tilgang til denne informasjonen.

Tildeling og delegering av roller i tråd med tjenstlige behov
I spørreundersøkelsen spurte vi lederne om tildeling av rollene i Gat er i tråd med tjenstlig behov. Enhetslederne ble spurt om sin enhet, mens kommunaldirektører og kommunalsjefer ble spurt om sitt tjenesteområde.

Tabell 3: Antall kommunaldirektører, kommunalsjefer og enhetsledere som oppgir om tildelte roller i Gat er i tråd med tjenstlig behov

Spørsmål	Ja	Nei	Vet ikke
Spørsmål til kommunaldirektører og kommunalsjefer: Er rollene som er tildelt i Gat for enhetene på ditt tjenesteområde, i tråd med det tjenstlige behovet?	5	0	3

[24] Citrix er en programvareplattform for virtualisering som lar brukere få sikker, ekstern tilgang til applikasjoner, skrivebordsmiljøer og data fra hvilken som helst enhet. Citrix-løsningen er via en server. En server er en kraftig datamaskin som leverer ressurser, data, tjenester eller programmer til andre datamaskiner over et nettverk.

[25] Ansatte logger inn via en spesifikk URL som tilhører Trondheim kommune. En URL (Uniform Resource Locator) er den unike adressen eller "lenken" du skriver inn i nettleseren for å finne en spesifikk nettside på internett. Den fungerer som en digital adresse som forteller nettleseren nøyaktig hvor den skal hente innholdet fra.

Spørsmål til de 16 enhetslederne: Er rollene som er tildelt i Gat for din enhet i tråd med det tjenestelige behovet?	14	0	2

Fem av åtte kommunaldirektørene og kommunalsjefene har svart at rollene innenfor deres tjenesteområde er i tråd med tjenstlige behov. 14 av 16 enhetsledere og fem av åtte kommunaldirektører og kommunalsjefer har svart at rollene som er tildelt til ansatte i deres enhet er i tråd med tjenstlig behov. De øvrige fem ledere vet ikke om rollene er tildelt i henhold til tjenestelig behov.

Delegering og tildeling av konkrete roller i Gat
Spørsmål om delegering og tildeling av bestemte roller ble kun sendt til de 16 enhetslederne i undersøkelsen. De enhetslederne som har svart ja på spørsmålene fikk oppfølgingsspørsmål, blant annet om hvilke stillinger dette gjelder.

	Ja	Nei	Vet ikke
Har dere delegert rollen "Enhetsleder" i Gat til ansatte som ikke er enhetsleder?	4	12	0
Har dere delegert rollen "Avdelingsleder" i Gat til ansatte som ikke er avdelingsleder?	2	14	0
Har dere tildelt rollen "Bruker 1" i Gat til ansatte ved enheten?	14	2	0
Har dere tildelt rollen "Vaktansvarlig" i Gat til ansatte ved enheten?	14	1	1

Tabell 4: Antall enhetsledere som svarte på ulike spørsmål om delegering av roller

Delegering av"Enhetsleder"-rollen
Fire enhetsledere har svart at de har delegert rollen "Enhetsleder" til ansatte som ikke er enhetsledere.

De enhetslederne som har svart at de har delegert rollen "Enhetsleder" har fått oppfølgingsspørsmål om hvilke stillinger de har delegert rollene til. To enhetsledere har delegert rollen til en avdelingsleder hvor den ene avdelingslederen fungerer som stedfortreder. En enhet

har delegert rollen til GAT-koordinator. En enhet har delegert rollen til en person (ikke angitt stilling) som har hatt denne enhetslederrollen i en periode ved langvarig fravær eller avvikling av sommerferie.

Delegering av "Avdelingsleder"-rollen
To enhetsledere har delegert rollen "Avdelingsleder" til ansatte som ikke er avdelingsledere.

De enhetslederne som har svart at de har delegert rollen "Avdelingsleder" har fått oppfølgingsspørsmål om hvilke stillinger de har delegert rollene til. En enhet har delegert rollen til administrasjonsteamet. En enhet har delegert rollen ved langvarig fravær eller avvikling av ferie, men har ikke angitt hvilken stilling denne rollen er delegert til.

Tildeling av "Bruker1"-rollen
14 enhetsledere har tildelt rollen "Bruker1" til ansatte ved enheten.

Enhetsledere som har svart at de har tildelt rollen "Bruker1" til ansatte ved enheten har fått oppfølgingsspørsmål om hvilke stillinger som har fått tildelt rollen "Bruker1".

Svarene fra de 14 enhetslederne som har tildelt rollen "Bruker1", varierer. Fem enheter svarte at driftspersonell har fått tildelt denne rollen. De øvrige svarte at rollen er tildelt plasstillitsvalgt, koordinator og HR-team, vaktansvarlig, fag, superbruker, helsesekretær/merkantil, teamledere, Gat-ansvarlige, ansatte med planansvar, konsulenter i administrative team og avdelingsleder.

De 14 enhetslederne har også fått tilleggsspørsmål om hva som var begrunnelsen for tildelingen.

Begrunnelsen for hvorfor de ansatte trenger denne rollen "Bruker1" varierer, men de fleste svarene omhandler at de må ha en vaktansvarlig på hver vakt for å kunne godkjenne turnuser, følge opp vaktbok, godkjenne timelister, registrere fravær, leie inn vikarer og tildele vakter ved fravær.

Enhetslederne har fått spørsmål om hvor mange ved deres enhet som har fått denne rollen.

Tildelingen av rollen "Bruker1" for de 14 enhetene, varierer mellom to og 30 personer for ti av disse enhetene. For de fire resterende enhetene svarte en enhetsleder at alle driftsansvarlige pluss noen enkelte ansatte har fått rollen "Bruker1" for å kunne få den daglige driften til å fungere. En enhetsleder svarte at ingen ansatte får denne rollen fast da de har fått tilbakemelding om at det er feil å tildele denne rollen. En enhetsleder er usikker på hvor mange ved enheten som er tildelt denne rollen, og en enhetsleder har ikke svart på spørsmålet.

Tildeling av vaktansvarlig-rollen
14 enhetsledere svarte at de har tildelt rollen "Vaktansvarlig" til ansatte på enheten.

Disse 14 enhetslederne har fått oppfølgingsspørsmål om hvilke stillinger som har fått tildelt denne rollen. Sju av disse enhetslederne oppga at rollen er tildelt sykepleiere, vernepleiere og eventuelt helsefagarbeidere. De øvrige enhetslederne svarte at rollen var tildelt "store stillinger", vaktansvarlige, tillitsvalgte og ulike stillinger som har ansvarsvakt. En enhetsleder svarte at de er pålagt å ha en vaktansvarlig på hver vakt, noe som betyr at alle faggrupper i prinsippet kan ha rollen "Vaktansvarlig". En enhetsleder svarte at rollen er avviklet og erstattet med "MinGatLeder". En annen enhetsleder svarte at ansatte som har deltatt på opplæring er tildelt denne rollen.

De samme 14 enhetslederne har fått oppfølgingsspørsmål om hva som er begrunnelsen for tildelingen av rollen "Vaktansvarlig". Begrunnelsen for hvorfor de ansatte trenger denne rollen varierer, men de fleste svarene omhandler at de må ha en vaktansvarlig på hver vakt for å kunne godkjenne turnuser, registrere fravær, leie inn vikarer og tildele vakter ved fravær. En enhetsleder svarte at alle i fast stilling i turnus hadde fått tildelt rollen "Vaktansvarlig" for å legge inn fravær og leie inn vikar, men at dette nå var endret til "MinGatLeder".

De samme 14 enhetslederne har også fått tilleggsspørsmål om hvor mange ved enheten deres som har fått rollen"Vaktansvarlig". I svarene varierer det mellom 17 og 150 personer for ti av enhetene. Tre av de andre enhetsledere svarte at de var usikre på hvor mange ved deres enhet som er tildelt denne rollen og en enhetsleder har ikke svart på spørsmålet.

Administrator rolle
Vi har sett at det er tildelt sju administrator roller i Gat i Trondheim kommune. En av disse var en enhetsleder. Vi har ved verifisering av denne rapporten fått opplyst fra tjenesteforvalter at denne enhetslederen nå er fratatt rollen.

Citrix-lisenser for Gat
Som nevnt i forrige kapittel så eksisterer det to versjoner av systemet Gat, med ulike typer tilganger og roller. Tilganger til Gat kan gis direkte til server via en Citrix-løsning. Enhetene må betale for Citrix-lisensene.

Spørsmålene om Citrix-lisenser for Gat til ansatte er bare sendt til enhetslederne, ikke til kommunalsjefene og kommunaldirektørene.

Spørsmålet om Citrix-lisenser til enheter på tjenesteområdene er bare sendt til kommunalsjefene, ikke til enhetslederne eller kommunaldirektørene.

Tabell 4: Antall enhetsledere og kommunalsjefer som oppgir at det er bestilt nye Citrix-lisenser etter overgangen til webversjonen av Gat

	Ja	Nei	Vet ikke
Spørsmål til enhetsledere: Har enheten bestilt nye Citrix-lisenser etter overgangen til webversjonen av Gat?	7	2	7
Spørsmål til kommunalsjefer: Har enhetene på ditt tjenesteområde bestilt nye Citrixlisenser etter overgangen til webversjonen av Gat?	1	0	5

Sju enhetsledere svarte at enhetene har bestilt nye Citrix-lisenser etter overgangen til webversjonen av Gat. Disse sju fikk tilleggsspørsmål om hva som var årsaken til at Citrix-lisenser ble bestilt. Sju enhetsledere vet ikke om det er bestilt Citrix-lisenser til sin enhet.

De som svarte at de har bestilt nye Citrix-lisenser etter overgangen til webversjonen av Gat, oppgir ulike årsaker til dette. En enhetsleder svarte at det var behov for rollen "Vaktansvarlig" i Citrix-løsningen for å få bedre oversikt over tilgjengelige ressurser og for å kunne tildele vakter. En

enhetsleder svarte at de bestilte Citrix-lisens slik at noen utvalgte ansatte kunne ha mulighet til å leie inn personell og flytte ansatte mellom avdelingene. En enhet svarte at de først hadde fått fjernet alle Citrix-lisensene, men da ble det utfordrende å drifte enheten. De bestilte derfor Citrix lisens til noen dedikerte ansatte. Øvrige forklaringer er at det er bestilt Citrix-lisens til nyansatte sykepleiere eller at det var vurdert som nødvendig med Citrix-lisens. En av enhetslederne har ikke beskrevet årsaken.

De sju enhetslederne fikk også tilleggsspørsmål om hvor mange Citrix-lisenser som ble bestilt til enheten. En enhet har bestilt Citrix-lisens til alle sykepleiere og vernepleiere på enheten. En enhet har bestilt ti Citrix-lisenser. En enhet har bestilt fem lisenser, to enheter har bestilt tre og en enhet har bestilt en Citrix-lisens. En enhetsleder har ikke oppgitt antallet.

Revisjonens vurderinger

Revisjonen mener det er en risiko at så mange ansatte ved enkelte enheter i kommunen er tildelt rollen “Bruker1”, som har utvidede rettigheter. 14 av 16 forespurte enhetsledere har fordelt denne rollen til mellom to og 30 ansatte ved sin enhet. Vi har som tidligere nevnt sett at rollen “Bruker1” har blitt brukt i forbindelse med misligheter. Revisjonen ber byrådet vurdere behovet for at så mange ansatte skal ha tilgang til denne rollen.

Revisjonen mener også det er en risiko at 14 av de 16 enhetene i denne undersøkelsen har tildelt rollen “Vaktansvarlig”, som også har utvidede rettigheter til mellom 17 og 150 personer ved sine enheter. Vi ber Byrådet vurdere behovet for at så mange ansatte har rollen "Vaktansvarlig".

Rollen “Vaktansvarlig” finnes kun i Citrix-versjonen av Gat og krever Citrix-lisenser for hver bruker. Rollen skulle etter det revisjonen har fått opplyst kunne erstattes av rollen “MinGatLeder” i web-versjonen. Sju enhetsledere har i spørreundersøkelsen svart at enhetene har bestilt nye Citrix-lisenser etter overgangen til web-versjonen av Gat på grunn av at rollen “MinGatLeder” i web-versjonen ikke dekker behovet til enhetene. Revisjonen mener byrådet bør vurdere om rollen “MinGatleder” i web-versjonen kan tilpasses behovet hos enhetene med tilstrekkelige rettigheter slik at kommunen kan spare kostnader for Citrix-lisenser.

Revisjonen mener det er en risiko at rollene “Enhetsleder” og “Avdelingsleder” er delegert til ansatte som ikke er enhetsleder eller avdelingsleder. Disse rollene gir full registreringstilgang til egen enhet, og både enhetsleder og avdelingsleder kan anvise på timelistene.

Revisjonen mener byrådet bør vurdere om delegering av rollene “Enhetsleder”, “Avdelingsleder”, “Vaktansvarlig” og “Bruker1” er i henhold til prinsippet om minst mulig privilegium. Ansatte skal kun ha tildelt de rollene de trenger for å utføre sine arbeidsoppgaver. Byrådet bør vurdere om de rollene som er opprettet i Gat tilfredsstiller behovene til enhetene uten at de ansatte får for vide rettigheter i systemet.

Revisjonen mener det er en risiko at rollen “Administrator” gir mulighet til å tildele enkeltrettigheter direkte til ansatte, utover de rettighetene som ligger i de rollene ansatte er tildelt i Gat. Det er kun administratorer som har mulighet for å gi ansatte slike tilleggsrettigheter og som har tilgang til og oversikt over slike tilleggsrettigheter. Enhetene selv har ikke innsyn i disse tilleggsrettighetene. Det medfører en risiko for at ansatte har tilganger og rettigheter, utover sine tildelte roller i Gat, som lederne ikke er kjent med. Revisjonen anbefaler at rollene i Gat justeres eller at det opprettes nye roller slik at alle nødvendige rettigheter blir gitt innenfor en definert

rolle og dermed er kjent for lederne. Slike tilleggsrettigheter gis ifølge tjenesteforvalter kun på bestilling fra enhetsleder, som er autorisert bestiller. Revisjonen mener det er en risiko at rollen "Administrator" har vært tildelt en enhetsleder. Revisjonen mener dette er uforenelig med å være enhetsleder med anvisningsmyndighet.

Revisjonen registrerer at 19 av 24 forespurte ledere har svart at rollene som er tildelt ansatte ved deres ansvarsområde er i tråd med det tjenstlige behovet. Revisjonen mener likevel det er en risiko at så mange ansatte i kommunen er tildelt rollene "Bruker1" og "Vaktansvarlig" som begge har utvidede rettigheter. Revisjonen ber om en tilbakemelding på om risikoen ved at så mange ansatte har utvidede roller i Gat er vurdert. Vi ber også om en vurdering av om alle som har disse rollene har tjenstlig behov i henhold til prinsippet om minst mulig privilegium.

3.4 Rutiner for tilgangshåndtering for Gat

Kommunen har to sentrale skriftlige rutiner for å tildele, endre og slette tilganger i Kvaliteket . Den ene rutinen er "IT-utmelding for enhetsledere" (ID:6028-5). Denne skal sikre at tilganger og anvisningsmyndighet avsluttes ved sluttdato. Rutinen beskriver at roller i fagsystemer, eksempelvis "Gat anviser", må avsluttes når en enhetsleder slutter i stillingen. Den andre rutinen i Kvaliteket er "IT-tilganger i Trondheim kommune" (ID: 15741-6). Denne rutinen beskriver at sletting av tilgang i TK-nett må bestilles av en autorisert bestiller ved enheten. Dette skal gjøres i skjemaet "Ansatte slutter på enhet".

I spørreundersøkelse har vi videre spurt de 24 lederne følgende spørsmål:

Tabell 5: Antall ledere som oppgir at kommunen har retningslinjer i Gat

	Ja	Nei	Vet ikke
Har kommunen retningslinjer for tildeling av roller i GAT?	16	0	8
Har kommunen retningslinjer for sletting/avslutning av ansattes tilganger?	16	0	8

16 ledere har svart at kommunen har retningslinjer for tildeling og sletting av tilganger, mens de øvrige åtte lederne (to kommunaldirektører, tre kommunalsjefer og tre enhetsledere) vet ikke om kommunen har slike retningslinjer.

De 16 lederne som har svart at de har retningslinjer for tildeling av roller i Gat har fått tilleggsspørsmål om hvilke retningslinjer som ligger til grunn for dette. Lederne gir ulike svar på hvilke retningslinjer dette er. Noen viser til at rutiner ligger i Kvaliteket, at kommunen har bestillingsskjema for å søke om tilganger eller at tilganger bestilles av autorisert bestiller. En har vist til flere rutiner i Kvaliteket og på kommunens intranett. En viser til at de har lokale rutiner og bruker autorisert bestiller.

16 ledere har svart at de har retningslinjer for sletting/avslutning av ansattes tilganger og disse har fått tilleggsspørsmål om hvilke retningslinjer dette er. Her er det også ulike svar. Noen viser til rutiner i Kvaliteket, blant annet rutine ”IT-utmelding for enhetsledere” (ID:6028-5). Denne skal sikre at tilganger og anvisningsmyndighet avsluttes ved sluttdato. Rutinen beskriver at roller i fagsystemer, eksempelvis “Gat anviser”, må avsluttes når en enhetsleder slutter i stillingen. En annen rutine i Kvaliteket er “IT-tilganger i Trondheim kommune” (ID: 15741-6) som beskriver at sletting av tilgang i TK-nett må bestilles via Selvbetjeningsportalen av en autorisert bestiller ved enheten. Dette skal gjøres i skjemaet “Ansatte slutter på enhet”.

Noen enhetsledere viser til lokale rutiner og bruk av Selvbetjeningsportalen utover de sentrale retningslinjene. En leder har svart at når ansatte slutter, avsluttes tilgangen til Gat gjennom at merkantile sender inn skjema til Gat-teamet. En annen har svart at stopp/sletting av tilgang og roller i Gat må bestilles både via skjemaet "Ansattilgang fagsystem" / "Ansatt slutter på enhet" og ERP tilgangsskjema i Selvbetjeningsportalen.

Revisjonen har observert at en enhetsleder innen helse og omsorg som sluttet i kommunen for ti år siden, fortsatt er tildelt en rolle som enhetsleder i Gat. Vedkommende har ikke tilgang til kommunens intranett, og vil derfor ikke ha tilgang til Gat. Dersom denne personen på nytt hadde blitt ansatt i kommunen i en annen stilling, kunne man risikere at den gamle rollen, med store rettigheter i Gat som ikke var fjernet, kunne bli tilgjengelig for vedkommende.

Revisjonens vurderinger

De mange ulike svarene på revisjonens spørsmål om kommunen har rutiner for tilgangshåndtering i Gat, kan tyde på at kommunen ikke har rutiner som spesielt omhandler tilgangshåndtering for dette systemet.

IT-systemet Gat er et stort system som i 2025 genererte variabel lønn på i overkant 400 millioner kroner for byrådsområder knyttet til turnusbaserte tjenester i kommunen. Det er ca 18 000 brukere av Gat. Det er derfor viktig at kommunen har kontroll på tilgangshåndtering i systemet.

Revisjonen anbefaler at det utarbeides felles retningslinjer for tilgangshåndtering til systemet Gat for å sikre at ansatte kun har tilgang til Gat i tråd med tjenstlig behov. Retningslinjen bør sikre at ansatte tildeles roller i Gat etter prinsippet om minst mulig privilegium, at roller endres eller fjernes når ansatte skifter stilling i kommunen og at roller fjernes når ansatte slutter i kommunen.

3.5 Evaluering av tilganger (roller/rettigheter) i Gat

I spørreundersøkelsen har vi spurt lederne om de har jevnlig evaluering av tilganger i Gat.

Tabell 6: Antall enhetsledere, kommunaldirektører og kommunalsjefer som svarer at de jevnlig evaluerer tilganger (roller/rettigheter) i Gat

	Ja	Nei	Vet ikke
Spørsmål til enhetsledere: Evaluerer enheten jevnlig tilganger (roller/rettigheter) i Gat?	7	7	2

Spørsmål til kommunaldirektører og kommunalsjefer: Evaluerer enhetene på ditt tjenesteområde jevnlig tilganger (roller/rettigheter) i Gat?	2	1	5

Sju enhetsledere har svart at de jevnlig evaluerer tilganger (roller/rettigheter). Disse enhetslederne har fått tilleggsspørsmål om hvilken type evalueringer som gjennomføres. En enhetsleder svarte at de evaluerer hvem som har behov for ulike tilganger (roller/rettigheter). En enhet svarte at de går gjennom tilganger ved ny tillitsvalgt og ved nytilsatte som bør ha "Vaktansvarlig" rollen. Fire enheter svarte at de har årlige gjennomganger av tilganger og roller.

Kommunalsjefen som svarte at de har jevnlig evaluering av tilganger/roller, har svart at de tar vekk tilganger til ansatte som ikke har tjenestelig behov. En kommunaldirektør svarte at de har jevnlig evaluering av tilganger/roller, men at dette ansvaret ligger hos virksomhetsområdet ved kommunalsjef. Fem kommunaldirektører eller kommunalsjefer vet ikke om enhetene på deres tjenesteområde jevnlig evaluerer tilganger i Gat.

Revisjonens vurderinger

Under halvparten av enhetene evaluerer jevnlig ansattes tilgang i Gat. Revisjonen anbefaler at det utarbeides retningslinjer for tilgangshåndtering til Gat der det inngår at enhetene jevnlig skal evaluere tilganger til roller i systemet. Dette er viktig for å sikre at ansattes rettigheter er i henhold til prinsippet om minst mulig privilegium. Revisjonen har ved tidligere undersøkelser sett at risikoen for feil er størst når ansatte skifter stilling internt i kommunen. Ansatte som skifter stilling internt, kan ta med seg for vide rettigheter i et IT-system dersom tilganger til systemene ikke jevnlig evalueres.

Revisjonen stiller spørsmål om det er mulig å legge opp en automatisk kontroll ("vasking") av tilganger i Gat mot tilganger i TK-nett.

3.6 Loggføring av bruken av Gat

Tjenesteforvalter for Gat har opplyst at alt man gjør i Gat logges knyttet opp til den identen de ansatte har i systemet. Administrator har tilgang til loggen, og ser på loggen eksempelvis ved mistanke om misligheter. Ved gjennomgang av loggen har man mulighet for å kunne undersøke og avklare hvem som har utført både eventuelle utilsiktede handlinger som feil og uhell, men også tilsiktede handlinger.

Enhetene har ifølge tjenesteforvalter ikke tilgang til logg som viser alle hendelser per ident, men de har tilgang til logging av avvik ved registrering av timer, fravær og overføringer til lønnssystemet.

Ingen ledere i spørreundersøkelsen har svart at enhetene jevnlig gjennomgår logger for å avdekke misbruk av roller. Én enhetsleder som likevel har svart at de jevnlig gjennomgår logger for eventuelt å avdekke misbruk av roller, svarte at de ved ledermøter sjekket at ansatte som har hatt sin siste dag på jobb, også har fått fjernet sine tilganger, deriblant tilgangen til Gat.

Logging i Gat kan brukes til å dokumentere hva som er gjort, når det er gjort, og hvem som har gjort det. Dette kan bidra til operasjonell og sikkerhetsmessig etterlevelse av lover, regler og interne rutiner.

Revisjonens vurderinger

Revisjonen mener det er positivt at alt man gjør i Gat logges og knyttes opp til den identen de ansatte har i systemet. Administrator har tilgang til loggen og ser på den eksempelvis ved mistanke om misligheter. Enhetene har ifølge tjenesteforvalter ikke tilgang til logg som viser alle hendelser per ident, men de har tilgang til logging av avvik ved registrering av timer, fravær og overføringer til lønnssystemet.

Revisjonen anbefaler at byrådet vurderer om enhetene kan benytte loggen i Gat for å avdekke eventuelle misbruk.

Gjennomgang av logger av bruken av IT-systemer er et viktig sikkerhetstiltak for å oppdage, forebygge og håndtere uønskede IKT-hendelser. Logging bidrar til å identifisere brudd på tilgangsstyring og gir oversikt over hvem som har gjort hva i systemene.

4 Opplæring og støtte

4.1 Revisjonskriterier

- Kommunen skal sørge for opplæring og støtte til de som bruker Gat.
- Kommunen bør sørge for opplæring av tjenesteforvalter i informasjonssikkerhet og personvern.

4.2 Opplæring og støtte ved bruk av Gat

I spørreundersøkelsen har vi sendt spørsmål om opplæring og støtte i bruken av Gat.

Tabell 8: Spørsmål til enhetslederne

	Ja	Nei	Vet ikke
Har du fått tilstrekkelig opplæring i bruk av Gat?	11	4	1
Har ansatte ved din enhet som bruker Gat fått tilstrekkelig opplæring i systemet?	12	1	3
Får enheten tilstrekkelig støtte i bruk av Gat?	13	0	3

Tabell 9: Spørsmål til kommunalsjefene og kommunaldirektørene

	Ja	Nei	Vet ikke

Har ansatte som bruker Gat på ditt område fått tilstrekkelig opplæring i systemet?	1	0	7
Får enhetene på ditt område tilstrekkelig støtte i bruk av Gat?	2	0	6

De fleste enhetslederne svarte at de og deres ansatte hadde fått tilstrekkelig opplæring i systemet Gat. Fire av 16 enhetsledere svarte at de selv ikke hadde fått tilstrekkelig opplæring. Tre enhetsledere visste ikke om deres ansatte hadde fått tilstrekkelig opplæring i Gat. Sju av de åtte kommunaldirektørene og kommunalsjefene visste ikke om ansatte på deres område hadde fått tilstrekkelig opplæring i Gat.

13 av de 16 enhetsledere svarte at de får tilstrekkelig støtte i bruken av Gat, mens tre enhetsledere ikke vet om enheten får tilstrekkelig støtte.

Seks av åtte kommunaldirektører og kommunalsjefer svarte at de ikke vet om enhetene på deres område har fått tilstrekkelig støtte i bruk av Gat.

Vi stilte i spørreundersøkelsen følgende tre åpne spørsmål til de 24 lederne som deltok:

1. Beskriv eventuelle mangler eller forbedringspunkter i opplæringen i bruk av Gat:

15 ledere har lagt inn kommentarer på dette spørsmålet. Åtte svarte at de ikke har forutsetning for å svare på dette. De øvrige sju har nevnt følgende forhold:

- Det er tungvint å sjekke om innleie utløser brudd på arbeidsmiljøloven eller overtid. Det fører til "lettvinte" løsninger som ikke nødvendigvis er de beste.
- Desentraliserte tjenestesteder med lav ledertetthet har stort behov for at mange ansatte har rollene “Bruker1” og “Vaktansvarlig”.
- Det er krevende å gi riktig og god nok opplæring, og det gir en kontrollutfordring.
- Man kan bli mer konkret i forbindelse med utarbeidelse av turnus.
- Ønsker standardiserte brukermanualer i Min Gat og Gat.
- Det er fint med opplæringsdager.
- Enhetsleder burde fått bedre opplæring.

2. Hva er årsaken til at dere eventuelt opplever manglende støtte i bruk av Gat?

Ingen av de 24 lederne kom med tilbakemelding om at de opplevde manglende støtte i bruk av Gat.

3. Har du andre kommentarer til bruk av Gat?

To ledere kommenterte at systemet Gat er tregt. De blir ofte "kastet" ut og bruker lang tid på å koble seg opp. Lederen innen byutvikling svarte at de trenger en link fra Gat til timeføring i HR portalen. De oppga at de møter liten forståelse for dette, men at det er helt essensielt for virksomheten deres.

Revisjonens vurderinger

Revisjonen mener det er positivt at de fleste av de 16 enhetslederne i spørreundersøkelsen svarte at de selv og deres ansatte har fått tilstrekkelig opplæring i Gat. Sju av åtte kommunaldirektører

og kommunalsjefer svarte at de ikke vet om de ansatte på sitt område har fått tilstrekkelig opplæring.

Revisjonen mener det er positivt at 13 av 16 enhetsledere svarte at de får tilstrekkelig støtte i bruken av Gat. Ingen av de 24 i spørreundersøkelsen kommenterte i det åpne spørsmålet at de opplevde manglende støtte i bruken av Gat.

Det var lite øvrige kommentarer til bruken av Gat i spørreundersøkelsen, men det kan se ut som om noen enheter jobber litt tyngre med bruken av systemet.

Revisjonen stiller spørsmål om det innenfor systemet Gat er mulig å finne en løsning som kan oppfylle behovet innen Byutvikling. Vi ber også om en vurdering av responstiden til Gat fordi enkelte enheter opplever systemet som "tregt".

4.3 Informasjonssikkerhet og personvern

Kommunen bør sørge for opplæring av tjenesteforvalter i informasjonssikkerhet og personvern. Vi har i møte med tjenesteforvalter for Gat stilt spørsmål om hun har fått opplæring i informasjonssikkerhet og personvern.

Informasjonssikkerhet:

De sentrale komponentene i informasjonssikkerhet for et IT-system er:

- Konfidensialitet: Sikrer at informasjon kun er tilgjengelig for autoriserte brukere.
- Integritet: Sikrer at informasjonen er korrekt, pålitelig og ikke utilsiktet endret.
- Tilgjengelighet: Sikrer at autoriserte brukere har tilgang til informasjonen når de trenger den.

Revisjonen har mottatt følgende informasjon fra tjenesteforvalter:

Konfidensialitet: Tjenesteforvalter opplyser at de sikrer konfidensialitet i Gat ved at det er opprettet flere tilgangsgrupper som styres av enhetsleder. Det er kun enhetsleder og avdelingsleder som har ferdig definerte tilganger som legges til automatisk ved import av stillingen fra HR.

Integritet: Tjenesteforvalter opplyser at dette er ivaretatt ved at mulighet for å utføre endringer i Gat i henhold til oppsatt regelverk er begrenset til få personer.

Tilgjengelighet: Tjenesteforvalter opplyser at dette er ivaretatt ved at tilgangsgruppene er tilrettelagt for funksjon.[26]

Personvern
EUs personvernforordning GDPR (General Data Protection Regulation) trådte i kraft i Norge 20. juli 2018 gjennom den nye personopplysningsloven. Regelverket styrker individets personvern og gir virksomheter strenge plikter ved behandling av personopplysninger. Brudd på personopplysningsloven kan medføre store bøter.

[26] Den funksjonen de har i enheten, eksempelvis at ledernivå kan anvise lønn mens merkantil kan attestere lønn

Tjenesteforvalter opplyser at det har vært stort fokus på GDPR og personvern etter at personopplysningsloven trådte i kraft i 2018.

Revisjonens vurderinger

Det er positivt at tjenesteforvalter opplyser at hun har fått opplæring i informasjonssikkerhet og at det har vært stort fokus på personvern.

5 Konklusjon

Har Trondheim kommune definert ansvar og oppgaver som tjenesteforvalter, tjenesteeier og byrådsområdene skal ha for IT-systemet Gat?

- De fleste lederne er usikre på om det finnes skriftlige rutiner for ansvarsfordeling mellom de fire ansvarsnivåene ved endringer eller nye roller i Gat.
- Kommunen har en detaljert rutine for tjenesteforvalter for daglig drift av Gat. Rutinen mangler en beskrivelse av hvordan roller i Gat skal vurderes løpende.

Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemet Gat for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk?

- Det er ingen lett tilgjengelig beskrivelse av hvilke rettigheter som inngår i de ulike rollene i Gat, noe som er nødvendig for at enhetene skal kunne bestille riktige roller.
- Det er en risiko at rollen "Merkantil" attesterer og dermed bekrefter at registrerte timer i Gat stemmer med utført arbeid. Merkantilt personale kan i mange tilfeller ha for lite kjennskap til om timene er korrekte.
- Det er en risiko at så mange ansatte i kommunen har rollene "Bruker1" og "Vaktansvarlig" med utvidede rettigheter som kan være ut over tjenestlig behov.
- Rollen “Vaktansvarlig” brukes fortsatt i Citrix-versjonen fordi erstatningsrollen “MinGatLeder” i web-versjonen ikke tilfredsstiller enhetenes behov, noe som medfører ekstrakostnader for Citrix-lisenser.
- Det er en risiko når rollene “Enhetsleder” og “Avdelingsleder” delegeres til ansatte som ikke innehar disse lederstillingene. Disse rollene gir full registreringstilgang til egen enhet, og både enhetsleder og avdelingsleder kan anvise på timelistene.
- Rollen “Administrator” kan tildele enkeltrettigheter utover tildelte roller, og enhetsledere har ikke innsyn i disse tilleggsrettighetene. Ansatte kan derfor ha tilganger og rettigheter i Gat, som lederne ikke er kjent med.
- Kommunen har ikke rutiner som spesielt omhandler tilgangshåndtering for Gat.
- Færre enn halvparten av enhetene evaluerer jevnlig ansattes tilgang i Gat, noe som er viktig for å følge prinsippet om minst mulig privilegium.
- Alle handlinger i Gat logges, og administrator har tilgang til den fulle loggen, men enhetene har kun tilgang til logging av avvik ved registrering av timer, fravær og overføringer til lønnssystemet.

Har kommunen sikret opplæring og støtte til de som bruker Gat?

- De fleste av de 16 enhetslederne svarte at de selv og deres ansatte hadde fått tilstrekkelig opplæring i Gat.
- Sju av åtte kommunaldirektører og kommunalsjefer svarte at de ikke visste om de ansatte på deres område hadde fått tilstrekkelig opplæring.
- Et flertall av enhetslederne (13 av 16) svarte at de får tilstrekkelig støtte i bruken av Gat.
- Ingen av de 24 spurte kommenterte manglende støtte i det åpne spørsmålet i undersøkelsen.
- Tjenesteforvalter har fått opplæring i informasjonssikkerhet og det har vært stort fokus på personvern.

Ut fra konklusjonen på de tre problemstillingene så har kommunen ikke tilfredsstillende kontroll og oppfølging av turnussystemet Gat. Rapporten viser flere svakheter, spesielt knyttet til definering av ansvar og styring av roller og tilganger.

6 Byrådets uttalelse

TRONDHEIM KOMMUNE
Tråanten tjïelte

Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 TRONDHEIM

Vår saksbehandler	Vår ref.	Deres ref.	Dato
Øystein Døhl	2025/19787 oppgis ved alle henvendelser		01.06.2026

Høring - Etterlevelseskontroll IT - Gat turnussystem

Trondheim kommunerevisjon overleverte sin Rapport 3/2026 - RE Etterlevelseskontroll IT - Gat turnussystem 19.05.2026. Trondheim kommune ved Finansbyråd Lars Magnussen vurderer at revisjonsrapporten adresserer et tydelig og kjent utfordringsbilde i tilgangsstyring. Byråden har behandlet høringen og legger følgende punkter til grunn i høringsinnspillet

Svar på revisjonens vurderinger:

1. Rutiner for fordeling av ansvar:

Fra revisjonen: "Undersøkelsen viser at de fleste lederne ikke vet om det finnes skriftlige rutiner og retningslinjer for fordeling av ansvar mellom de fire ansvarsnivåene ved behov for nye roller eller endringer i eksisterende roller i Gat. Slik vi gjorde i etterlevelseskontrollen i 2024 anbefaler vi på nytt at det etableres skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen. Disse rutinene/retningslinjene bør beskrive ansvarsfordelingen for innholdet i rollene i Gat mellom de fire ansvarsnivåene."

Svar:

- Byråden mener at det foreligger en beskrivelse på de ulike roller i Ansattportalen, Intranett, "Ny ansatt på enhet og Ansatt slutter på enhet" samt rutine i Kvaliteket Rutine 4240-1 "Ansatt slutter på enhet evt. også helt i kommunen". Byråden støtter at utdyping og påminnelse av rutinene vil være hensiktsmessig, og at alle berørte enheter vil få rutiner og oppgavebeskrivelser tilsendt samt at det i samarbeid med HR enheten vil bli et tema i lederopplæring

2. Skriftlige retningslinjer for tjenesteforvalter sitt ansvar:

"Etter revisjonens vurdering bør det framgå av rutinen hvem som skal beslutte endringer i innhold og rettigheter i de ulike rollene og om det eventuelt bør opprettes nye roller ved endrede behov."

Svar:

- Byråden tar punktet til etterretning og støtter at det bør foreligge en rutine som beskriver hvem som kan beslutte endringer på eksisterende roller, samt opprettelse av nye roller.

3. Kontroll med roller og tilganger til GAT:

Vi har plukket ut følgende punkter fra revisjonens vurderinger

kap 3.2 Roller i Gat er i samsvar med kommunens behov og betryggende sikkerhet

"Revisjonen mener det er uheldig at det ikke finnes en lett tilgjengelig beskrivelse av hvilke rettigheter som inngår i de ulike rollene i Gat."

Svar:

- Byråden støtter at det bør foreligge en lett tilgjengelig oversikt over rettigheter som inngår i de ulike rollene

"Revisjonen anbefaler at det utarbeides eller gjøres tilgjengelig en beskrivelse av hvilke rettigheter som inngår i de ulike rollene i Gat."

Svar:

- Byråden tar anbefalingen til etterretning, og det vil utarbeides en oversikt som publiseres for enhetene

"Revisjonen mener det er en risiko at det er rollen "Merkantil" som kan attestere timelister. Den som attesterer skal bekrefte at de registrerte timene i Gat stemmer med utført arbeid. Vi vurderer at merkantilt personale i mange tilfeller kan ha for lite kjennskap til timene for å kunne attestere."

Svar:

- Byråden støtter at "Merkantil" rollen ikke har den samme oversikten som de som gjør registreringer i Gat for en kvalitetskontroll før lønnsoverføring. Kompetansen knyttet til avhengigheten i fagprogrammene og lønnskompetanse ligger idag hos merkantil og ikke hos de som utfører de registreringene. Den totale forståelsen er viktig for å korrigere transaksjoner som avvises pga. feil i kontosegment må utføres av "Merkantil" da disse har kompetanse og forståelse av avhengighetene. Opplæring av avdelingsledere slik at attesteringen slik at den avhenighetsforståelsen i større grad vil være kompetanse hos "Avdelingsleder" rollen vil være et tiltak for å bedre kvaliteten på attesteringen før den går til anvisning.

"Revisjonen anbefaler at byrådet vurderer om dagens roller i Gat dekker enhetenes behov uten at ansatte får for omfattende rettigheter i systemet. Mange ansatte i kommunen har rollene

"Bruker1" og "Vaktansvarlig" som begge gir utvidede tilganger. Byrådet bør vurdere om rollene i Gat kan justeres, eller om det bør opprettes nye roller i systemet. Dette er nødvendig for å sikre at rollene er i samsvarer med kommunens behov og ivaretar betryggende sikkerhet."

Svar:

- Byråden støtter at omfanget av rollen "Bruker1" kan reduseres, vi vil vurdere omfanget på nytt

Kap 3.3 Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium

Revisjonen mener det er en risiko at så mange ansatte ved enkelte enheter i kommunen er tildelt rollen "Bruker1", som har utvidede rettigheter. 14 av 16 forespurte enhetsledere har fordelt denne rollen til mellom to og 30 ansatte ved sin enhet. Revisjonen ber byrådet vurdere behovet for at så mange ansatte skal ha tilgang til denne rollen.

Svar:

- Rettighetene i "Bruker1" er i stor grad tildelt de som arbeider med planer, utarbeidelse og vedlikehold. Endringer i organiseringen ved en sentralisering av bemanningsplanlegging vil gjøre det mulig å redusere antallet "Bruker1" ute på enhetene da disse oppgavene utføres sentralt. Byråden vil ta en gjennomgang av "Bruker1" tilgangene:

Revisjonen mener også det er en risiko at 14 av de 16 enhetene i denne undersøkelsen har tildelt rollen "Vaktansvarlig", som også har utvidede rettigheter til mellom 17 og 150 personer ved sine enheter. Vi ber Byrådet vurdere behovet for at så mange ansatte har rollen "Vaktansvarlig".

Svar:

- Byråden mener at rollen "MinGat Leder" er tilstrekkelig for at de ansatte som registrerer fravær og innleie ved avvik fortrinnsvis utenfor normalarbeidstiden er tilstrekkelig.
- Byråden mener at tildelingen av rollene "Enhetsleder og Avdelingsleder", som er i henhold til de roller disse gruppene har i HR, er i henhold til beskrivelsen av deres oppgaver knyttet til anvisning av lønn

"Revisjonen mener byrådet bør vurdere om rollen "MinGatleder" i web-versjonen kan tilpasses behovet hos enhetene med tilstrekkelige rettigheter slik at kommunen kan spare kostnader for Citrix-lisenser. "

Svar:

- Byråden støtter revisjonens vurderingen her, men så langt er det den enkelt enhetes vurdering som legges til grunn når tilganger bestilles. Funksjonaliteten i "MinGatleder" er knyttet til daglig ajour av den planlagte arbeidstiden. Som kommentert i punktet ovenfor er det enhetene som ønsker at enkelte "Vaktansvarlige" skal ha utvidet mulighet for korrigeringer av den faktiske arbeidstiden - dvs. korrigere vakter, opprettet vakter utover det som er planlagt behandle merarbeid som avlønnes i henhold til overtidsbestemmelsene i Hovedtariffavtalen

"Revisjonen mener det er en risiko at rollene "Enhetsleder" og "Avdelingsleder" er delegert til ansatte som ikke er enhetsleder eller avdelingsleder. Disse rollene gir full registreringstilgang til egen enhet, og både enhetsleder og avdelingsleder kan anvise på timelistene. Revisjonen mener byrådet bør vurdere om delegering av rollene "Enhetsleder", "Avdelingsleder", "Vaktansvarlig" og "Bruker1" er i henhold til prinsippet om minst mulig privilegium. Ansatte skal kun ha tildelt de rollene de trenger for å utføre sine arbeidsoppgaver. Byrådet bør vurdere om de rollene som er opprettet i Gat tilfredsstiller behovene til enhetene uten at de ansatte får for vide rettigheter i systemet."

Svar:

- Byråden støtter bekymringen knyttet til delegering av roller som kan anvise lønn. Bakgrunn for dagens praksis er å sikre at utlønning ikke stopper opp, eksempelvis ved fravær fra leder. Byrådens vurdering er at systemets oppbygging ved flere nivå for attestasjon og anvisning vil ivareta at ikke samme person har begge funksjonene og at kontroll er mulig

"Revisjonen mener det er en risiko at rollen "Administrator" gir mulighet til å tildele enkeltrettigheter direkte til ansatte, utover de rettighetene som ligger i de rollene ansatte er tildelt i Gat. Det er kun administratorer som har mulighet for å gi ansatte slike tilleggsrettigheter og som har tilgang til og oversikt over slike tilleggsrettigheter. Enhetene selv har ikke innsyn i disse tilleggsrettighetene. Det medfører en risiko for at ansatte har tilganger og rettigheter, utover sine tildelte roller i Gat, som lederne ikke er kjent med. Revisjonen anbefaler at rollene i Gat justeres eller at det opprettes nye roller slik at alle nødvendige rettigheter blir gitt innenfor en definert rolle og dermed er kjent for lederne. Slike tilleggsrettigheter gis ifølge tjenesteforvalter kun på bestilling fra enhetsleder, som er autorisert bestiller. Revisjonen mener det er en risiko at rollen "Administrator" har vært tildelt en enhetsleder. Revisjonen mener dette er uforenelig med å være enhetsleder med anvisningsmyndighet. "

Svar:

- Byråden er klar over risikoen, men ingen rettigheter enten det er roller eller personlige utover dette tildeles med mindre det foreligger en bestilling i Ansattportalen fra autorisert bestiller. Bestilles det personlige rettigheter på autorisert bestiller er det dialog med enhetsleder før disse tildeles

kap 3.4 Rutiner for tilgangshåndtering for Gat

"De mange ulike svarene på revisjonens spørsmål om kommunen har rutiner for tilgangshåndtering i Gat, kan tyde på at kommunen ikke har rutiner som spesielt omhandler tilgangshåndtering for dette systemet.

Revisjonen anbefaler at det utarbeides felles retningslinjer for tilgangshåndtering til systemet Gat for å sikre at ansatte kun har tilgang til Gat i tråd med tjenstlig behov. Retningslinjen bør sikre at ansatte tildeles roller i Gat etter prinsippet om minst mulig privilegium, at roller endres eller fjernes når ansatte skifter stilling i kommunen og at roller fjernes når ansatte slutter i kommunen. "

Svar:

- Byråden støtter prinsipper om at tildeling, endring og avslutning av roller må tydeliggjøres. Vil også påpeke at tilganger i Gat sikres ved den informasjon som ligger tilgjengelig i Ansatteportalen på "Ansatt begynner og Ansatt slutter" samt de rutiner som foreligger i Kvaliteket - se lenker nederst i dokument

Oppsummering:

Et program av denne dimensjon som har et krav til 24/7 oppetid, samt at enheten til enhver tid skal ha en "levende" oversikt over hvilke ansatte som er tilstede på jobb krever en effektiv tilgangsstyring som byråden mener at kommunen pr. i dag har god kontroll på. Tilganger tildeles av Trondheim Digital, ERP, på bakgrunn av autorisert bestilling i Ansatteportalen.

Ansatteportalen beskriver funksjonaliteten i "Ansatt begynner og Ansatt slutter" godt, samt i Rutine ID:6006-7 IT-tilganger i Trondheim kommune fremkommer det hvordan tilganger skal opprettes/endres og slettes ved endring på stillingsforhold.

Rapportens pkt. 3.2 beskriver faren ved at det er avdekket et misbruk at rollen "Bruker1" som førte til feil og for mye utbetalt lønn, en ansatt misbrukte denne rollen tilbake i 2016 - 2017. Det er ikke mulig å fullstendig gardere seg mot mislighold, men byråden mener slike hendelser er ivaretatt ved at ingen variabellønn overføres til lønnssystemet uten at transaksjonen både er attestert og anvist.

Rapporten pkt. 3.3 Tildeling av "Bruker1" rollen beskriver at denne rollen har et tjenestelig behov da disse blant annet skal godkjenne turnuser og godkjenne timelister - dette medfører ikke riktighet da disse oppgavene er knyttet til rollene "Enhetsleder/Avdelingsleder og "Merkantil"

- Byråden støtter at en økt bruk av hendelser gjennom Logg i programmet kan gi god

oversikt over evt. uønskede IKT-hendelser
- Byråden støtter at programmet kan oppleves "tregt". Det jobbes kontinuerlig i samarbeid med programleverandøren, Trondheim digital og driftsleverandør for å optimalisere ytelsen

Byråden vil følge opp de punkter som er svart ut over i forbindelse med utarbeidelse av rutiner og retningslinjer

Ansatteportalen

IT-tilganger i Trondheim kommune

Kontroll på enhet før avslutt arbeidstaker skjema sendes

Med hilsen
Trondheim kommune

Olaf Løberg
finansdirektør

Øystein Døhl
økonomisjef

Dette er et digitalt dokument og har derfor ingen signatur

7 Revisjonen tilsvar på byrådets uttalelse

kap 2. Rutiner for fordeling av ansvar:

- Revisjonen registrerer at byråden svarer på beskrivelse av roller i ansattportalen. Revisjonens spørsmål gjelder fordeling av ansvar mellom tjenesteforvalter, tjenesteeier, byrådsområder og Trondheim digital når det gjelder behov for nye, eller endringer i eksisterende roller.

kap 3.2 Roller i Gat er i samsvar med kommunens behov og betryggende sikkerhet og Kap 3.3 Tildeling av roller i Gat skal følge prinsippet om minst mulig privilegium

- Revisjonen mener byråden sitt svar på om rollen "Merkantil" kan attestere timelister er uklart på hvem det er byråden mener skal ha ansvar for attestasjon av timelister.
- Byråden støtter at omfanget av rollen “Bruker1” kan reduseres, men revisjonen savner tilbakemelding på omfanget av rollen "Vaktansvarlig".
- Revisjonen registerer at byråden mener at rollen “MinGat Leder” er tilstrekkelig. Svarene revisjonen har mottatt på spørreundersøkelsen indikerer imidlertid at enhetene ikke deler denne oppfatningen. Vi savner en tilbakemelding på om det er mulig å endre rollen “MinGat Leder” slik at den er bedre tilpasset enhetens behov.

Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 Trondheim

www.trondheim.kommune.no/revisjon

Mars 2025
Forsidefoto:
Layout: Kommunikasjonsenheten

Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 Trondheim

www.trondheim.kommune.no/revisjon

Mars 2025
Forsidefoto:
Layout: Kommunikasjonsenheten