Til kontrollutvalget i Brønnøy kommune –
Tom Okan, leder
Birgitte Brattebø, nestleder
Leon Aune, medlem
Lisbeth Holand, medlem
Kåre Knutsen, medlem

Gjenpart går til:
Ordfører (jf. kommuneloven § 6-1)[1]
Kommunerevisjonen (jf. kommuneloven § 24-3)[1]
Kommunedirektør (til orientering – jf. kommuneloven § 13-1)[1]

Distribusjon pr. epost
Saksbehandler:
Sekretariatsleder
Tobias Langseth

INNKALLING TIL MØTE I KONTROLLUTVALGET

I samråd med utvalgets leder innkalles herved til møte som følger;

Dato: **Tirsdag 26. november**
Tid: **kl. 09:00 – 12:00**
Sted: Rådhuset [formannskapssal]

Til behandling:

Sak 21/2024 – Revisjonsstrategi [orientering fra regnskapsrevisor]
Sak 22/2024 – Møteplan for neste år [2025]
Sak 23/2024 – Agenda for virksomhetsbesøk [mars/2025]
Sak 24/2024 – Forvaltningsrevisjon og eierskapskontroll fremover
Sak 25/2024 – Aktuelle orienteringer fra sekretariatet
Sak 26/2024 – Eventuelt

Forfall meldes pr. telefon 909 62 145 eller epost.

Sandnessjøen 19.11.2024

Tobias Langseth (sign.)
Sekretariatsleder

[1]Utdrag fra kommuneloven:

§ 6-1. Ordførerens myndighet og oppgaver

Ordføreren har møte-, tale- og forslagsrett i alle kommunale eller fylkeskommunale folkevalgte organer unntatt kommune- og fylkesråd og organer under dem. I kontrollutvalget har ordføreren likevel bare møte- og talerett. Ordføreren har bare stemmerett i organer der han eller hun er valgt medlem. Ordføreren kan la et annet medlem av kommunestyret eller fylkestinget representere seg i de organene som han eller hun ikke er medlem av.

§ 13-1. Kommunedirektør. Myndighet og oppgaver

Kommunedirektøren har møte- og talerett i alle kommunale eller fylkeskommunale folkevalgte organer, med unntak av kontrollutvalget. Kommunedirektøren kan la en av sine underordnete utøve denne retten på sine vegne.

§ 24-3. Revisors møterett, opplysningsplikt mv.

Oppdragsansvarlig revisor eller hans eller hennes stedfortreder har møte- og talerett i kontrollutvalgets møter. Revisoren har rett til å få uttalelsene sine protokollert. Møteretten gjelder likevel ikke når en sak som angår en revisors tilsettingsforhold behandles.

Til kontrollutvalget i Brønnøy kommune Sandnessjøen 19.11.2024

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 21/2024: REVISJONSSTRATEGI [ORIENTERING FRA REGNSKAPSREVISOR]

1: Innledning og bakgrunn

Revisor har tatt initiativ til å holde en muntlig orientering for kontrollutvalget om revisjonsstrategi, herunder arbeidet med forenklet etterlevelseskontroll med økonomiforvaltningen etter reglene i kommuneloven § 24-9 [jf. appendiks].

2: Kontrollutvalgets oppgaver og rolle

Kontrollutvalgets oppgave er i denne omgang i hovedsak å danne seg et inntrykk av arbeidet med finansiell revisjon, jf. bestemmelsene i forskrift om kontrollutvalg og revisjon:

> **§ 3. Kontrollutvalgets oppgaver ved regnskapsrevisjon**
>
> Kontrollutvalget skal holde seg **løpende orientert** om revisjonsarbeidet og **påse** at
>
> a) kommunens eller fylkeskommunens årsregnskaper blir revidert på en betryggende måte
>
> b) regnskapsrevisjonen utføres i samsvar med lov, forskrift og kontrollutvalgets instrukser og avtaler med revisor
>
> c) regnskapsrevisjonen blir utført av revisorer som oppfyller kravene i kapittel 2 og 3.
>
> Kontrollutvalget skal uttale seg til kommunestyret eller fylkestinget om årsregnskapene og årsberetningene før formannskapet eller fylkesutvalget innstiller til vedtak.
>
> Kontrollutvalget skal påse at regnskapsrevisorens påpekinger etter kommuneloven § 24-7 til § 24-9 blir rettet eller fulgt opp. Hvis påpekingene ikke blir rettet eller fulgt opp, skal kontrollutvalget rapportere det til kommunestyret eller fylkestinget.

Forskrift om kontrollutvalg og revisjon - Lovdata

Det henvises for ordens skyld også til reglene for revisjon i kommuneloven kapittel 24:

Lov om kommuner og fylkeskommuner (kommuneloven) - Lovdata

3: Sekretariatets vurderinger

Det henvises til revisors redegjørelse i møtet, samt vedlagte uavhengighetserklæring.

Forslag til vedtak:

Kontrollutvalget tar revisors muntlige orientering om revisjonsstrategi til etterretning.

Vedlegg –
1: Uavhengighetserklæring datert 20.08.2024

APPENDIKS – Utdrag fra kommuneloven

§ 24-9. ***Forenklet etterlevelseskontroll med økonomi- forvaltningen***

Regnskapsrevisor skal se etter om kommunens eller fylkeskommunens økonomiforvaltning i hovedsak foregår i samsvar med bestemmelser og vedtak.

Revisor skal basere oppgaven på en risiko- og vesentlighetsvurdering, som skal legges fram for kontrollutvalget. Revisor skal innhente tilstrekkelig informasjon til å vurdere om det foreligger brudd på lover, forskrifter eller vedtak, der bruddet er av vesentlig betydning for økonomiforvaltningen.

Revisor skal senest 30. juni avgi en skriftlig uttalelse til kontrollutvalget, med kopi til kommunedirektøren, om resultatet av kontrollen.

Se også RSK 301 Standard for forenklet etterlevelseskontroll med økonomiforvaltningen:

RSK 301 Forenklet etterlevelseskontroll med økonomiforvaltningen - NKRF

IR.03 UA Joakim Bangstad 2024 Brønnøy kommune

Dokumentet er signert digitalt av følgende undertegnere:

- JOAKIM ANDRÉ BANGSTAD, signert 20.08.2024 med ID-Porten: BankID

Det signerte dokumentet innholder
• En forside med informasjon om signaturene
• Alle originaldokumenter med signaturer på hver side
• Digitale signaturer

Dokumentet er forseglet av Posten Norge
Signeringen er gjort med digital signering levert av Posten Norge AS. Posten garanterer for autentisiteten og forseglingen av dette dokumentet.

Slik ser du at signaturene er gyldig
Hvis du åpner dette dokumentet i Adobe Reader, skal det stå øverst at dokumentet er sertifisert av Posten Norge AS. Dette garanterer at innholdet i dokumentet ikke er endret etter signering.

Brønnøy kommune

Egenvurdering av uavhengighet

Kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon §16- §19 setter krav til revisors uavhengighet. Kravene er beskrevet i bestemmelsene. Dette dokumentet beskriver revisors egenvurdering og skal ivareta krav i forskriften.

Ansettelsesforhold	Undertegnede har ikke ansettelsesforhold i andre stillinger enn i revisjonsselskapet
Medlem i styrende organer	Undertegnede er ikke medlem i styrende organer i noen virksomhet som Brønnøy kommune deltar i.
Delta eller inneha funksjoner i annen virksomhet, som kan føre til interessekonflikt eller svekket tillit	Undertegnede deltar ikke i eller innehar funksjoner i annen virksomhet som kan føre til interessekonflikt eller svekket tillit til rollen som revisor.
Nærstående	Undertegnede har ikke nærstående som har en slik tilknytning til Brønnøy kommune at dette har betydning for min uavhengighet og objektivitet i utførelsen av revisjonsoppdraget.
Rådgivnings- eller andre tjenester som er egnet til å påvirke revisors habilitet	Undertegnede bekrefter at det ikke er ytet rådgivning eller andre tjenester overfor Brønnøy kommune som er av en slik art at dette kommer i konflikt med denne bestemmelsen. Før slike tjenester utføres, vurderer revisor rådgivningens eller tjenestens art i forhold til revisors uavhengighet og objektivitet. Dersom revisor konkluderer med at utøvelse av slik tjeneste kommer i konflikt med bestemmelsen i forskriftens § 16, utfører revisor ikke tjenesten. Hvert enkelt tilfelle vurderes særskilt. Revisor vil kunne besvare spørsmål/henvendelser som er å betrakte som veiledning og bistand og ikke revisjon. Slike veiledninger skjer med varsomhet og på en måte som ikke binder opp revisors senere revisjons- og kontrollvurderinger.
Tjenester under (fylkes)kommunens egne ledelses- og kontroll-oppgaver	Undertegnede bekrefter at det ikke ytes tjenester overfor Brønnøy kommune som hører inn under kommunens egne ledelses- og kontrolloppgaver.
Opptre som fullmektig for den revisjonspliktige	Undertegnede bekrefter at verken revisor eller Revisjon Midt-Norge SA opptrer som fullmektig for Brønnøy kommune.
Andre særegne forhold	Undertegnede kjenner ikke til andre særegne forhold som er egnet til å svekke tilliten til min uavhengighet og objektivitet.

Namsos, 20.08.24
Joakim Bangstad

Til kontrollutvalget i Brønnøy kommune Sandnessjøen 19.11.2024

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 22/2024: MØTEPLAN FOR NESTE ÅR [2025]

1: Innledning og bakgrunn

Av ulike årsaker ønsker de fleste kontrollutvalg å fastsette en møteoversikt.

2: Utkast til møteplan

Erfaringsmessig vil det som hovedregel være behov for minst 4 faste møter pr. år. I tillegg innkalles møter etter behov. Koordinering med andre kommuner og kontrollutvalg i samme geografiske område kan til en viss grad være ressurseffektivt med hensyn til møtedeltakelse som innebærer tidkrevende reisevirksomhet. Eksempelvis fra revisors side.

Ukedag **Onsdag**

Plan 2025	Brønnøy
Møte 1	12. mars
Møte 2	21. mai
Møte 3	24. september
Møte 4	26. november

Tidspunkt er vanligvis 08:30–12:00, og møtested vil normalt sett være rådhuset i Brønnøysund.

Aktuelle temaer/saker til behandling på møtene vil kunne være:

- Kontrollutvalgets årsrapport
- Gjennomgang av revisjonsstrategi
- Kontrollutvalgets uttalelse om årsregnskap og årsberetning
- Forenklet etterlevelseskontroll med økonomiforvaltningen
- Oppfølging av regnskapsrevisors påpekinger etter kommuneloven § 24-7 til § 24-9
- Bestilling av forvaltningsrevisjon og eierskapskontroll
- Rapporter fra gjennomført forvaltningsrevisjon og eierskapskontroll
- Oppfølging av tidligere forvaltningsrevisjon og eierskapskontroll
- Budsjett for kontrollarbeidet i kommunen
- Orienteringer fra administrasjonen og virksomhetsbesøk
- Enkeltstående kontrollsaker [eksempelvis henvendelser til kontrollutvalget]

3: Oppsummering og avslutning

Møteplan for 2025 fastsettes etter nærmere drøfting i kontrollutvalget.

Forslag til vedtak:

Forslaget til møteplan fastsettes som fremlagt [med de endringer som ble besluttet i møtet].

Til kontrollutvalget i Brønnøy kommune Sandnessjøen 19.11.2024

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 23/2024: AGENDA FOR VIRKSOMHETSBESØK

1: Innledning og bakgrunn

KDDs veileder om kontrollutvalgets rolle og oppgaver [3. utgave, kapittel 4] sier dette om «virksomhetsbesøk»:

Kontrollutvalsboka - regjeringen.no

Verksemdsbesøk

For å bli kjent med den kommunale forvaltninga og for at tilsette i kommunen skal bli kjende med kontrollutvalet, kan utvalet vitje ulike kommunale verksemder. Dette kan også omfatte kommunale føretak og selskap. Fleire kontrollutval har etablert ein slik praksis. Kontrollutvalet initierer og gjennomfører vitjingane i samarbeid med sekretariatet. Kor mykje arbeid som blir lagt ned i samband med desse vitjingane, kan tilpassast kva informasjon kontrollutvalet har bruk for, og korleis ressurssituasjonen deira er. Føremålet med verksemdsbesøk er mellom anna å

- bli kjent med verksemda og å gjere kontrollutvalsarbeidet kjent i kommunen
- undersøkje generelt om krav til internkontroll er kjende i verksemda, og om sentrale føringar knytte til til dømes etikk er kommuniserte
- sjekke utvalde område som til dømes HMT, offentlege anskaffingar og liknande ved å få orientering om og innsyn i system og rutinar
- få innspel til risikoanalysane og planarbeidet til kontrollutvalet

Se også: Veileder om kommunelovens internkontrollbestemmelser - regjeringen.no

2: Sekretariatets vurderinger

Det er avtalt virksomhetsbesøk hos kommunens tekniske avdeling 12. mars kl. 12:00–16:00 i etterkant av kontrollutvalgets møte. Kontrollutvalgets medlemmer har blitt invitert til å komme med innspill til tema/problemstillinger pr. epost. Jf. epostmelding til utvalget 9. og 17. oktober.

3: Oppsummering og avslutning

Agenda tas opp til diskusjon på møtet.

Forslag til vedtak:

Kontrollutvalget har diskutert aktuelle tema for orienteringene. Utvalgets forslag videreformidles kommunens administrasjon som ledd i forberedelsene til virksomhetsbesøket.

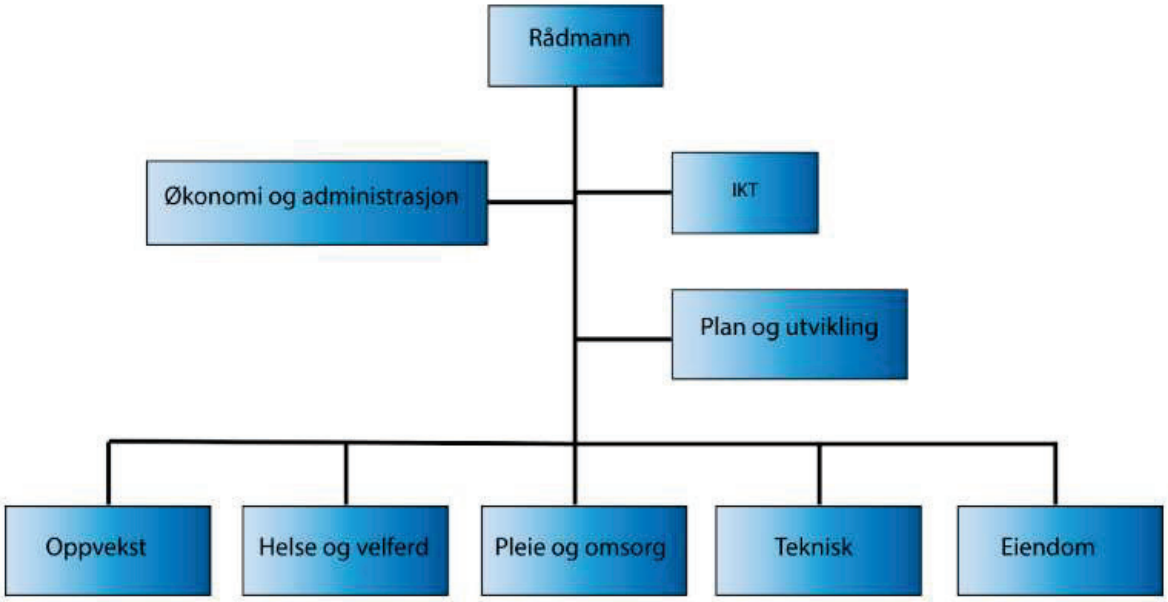
APPENDIKS – Organisering & tjenester teknisk avdeling

Organisasjon - Hovedportal

Organisasjon

Brønnøy kommune er organisert i 8 ulike virksomhetsområder, der rådmannen er øverste leder.

Mer informasjon om alle virksomhetsområdene vil komme etterhvert.



Sist endret: 26.03.2021 13.44

Teknisk, bolig og eiendom - Hovedportal

Til kontrollutvalget i Brønnøy kommune Sandnessjøen 19.11.2024

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 24/2024: FORVALTNINGSREVISJON OG EIERSKAPSKONTROLL FREMOVER

Innledning og bakgrunn

Utgangspunktet er planverket for forvaltningsrevisjon og eierskapskontroll [jf. appendiks 1]. Kontrollutvalget har fått fullmakt til å foreta endringer. Dermed er det mulig å avvike fra plan for forvaltningsrevisjon og eierskapskontroll, dersom det fremstår som formålstjenlig.

Utvalget foretok 12.03.2024 [sak 03/2024] bestilling av et forvaltningsrevisjonsprosjekt knyttet til «Barn med særlige behov, herunder flyktninger». I følge revisors prosjektplan, som ble behandlet av kontrollutvalget 11. juni [sak 09/2024], er rapport forventet levert innen 1. mars 2025.

Ressurshensyn tilsier at det er hensiktsmessig å foreta bestilling av et nytt prosjekt innen årsskiftet.

Sekretariatets vurderinger

Det anbefales i første omgang å prioritere gjennomføring av forvaltningsrevisjonsprosjekt knyttet til temaet «Informasjonssikkerhet og personvern». I tillegg til Brønnøy, har Sømna, Bindal og Vega kommune et tilsvarende prosjekt i planverket for forvaltningsrevisjon i valgperioden. De nevnte kommunene samarbeider i noen grad innenfor fagfeltet.

Som illustrasjon av hvordan et prosjekt kan være innrettet med henblikk på problemstillinger m.m., henvises det til følgende rapporteksempler fra andre kommuner:

Rennebu_2023_IKT_sikkerhet.pdf (nkrf.no)

Fauske_2022_Informasjonssikkerhet.pdf (nkrf.no)

Nord_Odal_2022_Informasjonssikkerhet.pdf (nkrf.no)

Bamble_2022_infosikkerhet_og_personvern.pdf (nkrf.no)

Namsos_2022_Infosikkerhet.pdf (nkrf.no)

Hamar_2022_Sikkerhetskultur.pdf (nkrf.no)

Personvern i skoler (nkrf.no)

Riksrevisjonen utfører nasjonale undersøkelser på ulike forvaltningsområder, eksempelvis:

Helseregistre: Ikke tilstrekkelig sikkerhet for person- og helseopplysninger (riksrevisjonen.no)

Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer (riksrevisjonen.no)

Undersøkelse av informasjonssikkerhet i Norfund (riksrevisjonen.no)

Oppsummering og avslutning

Revisjon Midt-Norge har utarbeidet et prosjektutviklingsnotat [jf. vedlegg 1], som kan danne grunnlag for kontrollutvalgets diskusjon i møtet.

Forslag til vedtak:

Kontrollutvalget bestiller et forvaltningsrevisjonsprosjekt knyttet til temaet «Informasjonssikkerhet og personvern». Utvalget ber om at Revisjon Midt-Norge utarbeider forslag til prosjektplan på basis av de signaler som fremkom, som legges frem for kontrollutvalget i egen sak.

Vedlegg –
1: Prosjektutviklingsnotat utarbeidet av RMN

Appendiks 1 – Plan for forvaltningsrevisjon og eierskapskontroll

A: Kontrollutvalgets forslag:

Kontrollutvalget har i møtene 12.03.2024, 11.06.2024 og 09.10.2024 drøftet revisors risiko- og vesentlighetsvurdering av kommunens virksomhet, virksomheten i kommunens selskaper samt kommunens eierskap – og legger med basis i denne analysen frem følgende forslag til uprioritert plan for hhv. forvaltningsrevisjon og eierskapskontroll i valgperioden:

PLAN FOR FORVALTNINGSREVISJON

Kommunens virksomhet

- Kommunens internkontrollarbeid
- IT-sikkerhet og personvern
- Planverket som styringsverktøy i kommunen

Virksomheten i kommunens selskaper

Foreslås nedprioritert av ressurshensyn.

PLAN FOR EIERSKAPSKONTROLL

- Helgeland Kraft AS

Merknad:
Prosjektet kan være aktuelt å gjennomføre parallelt med andre eierkommuner.

–//–

Planene for forvaltningsrevisjon og eierskapskontroll skal vedtas av kommunestyret selv.

Kontrollutvalget ber om at kommunestyret delegerer til kontrollutvalget å foreta endringer i planperioden, slik at utvalget selv kan foreta de prioriteringer utvalget finner nødvendig for gjennomføring av forvaltningsrevisjon og eierskapskontroll.

Kommunestyrets delegeringsadgang fremgår av kommuneloven §§ 23-3 og 23-4 tredje ledd.

Kontrollutvalgets forslag [innstilling] til kommunestyrevedtak er ut fra dette:

Kommunestyret slutter seg til kontrollutvalgets forslag til plan for forvaltningsrevisjon og eierskapskontroll i valgperioden.

Kommunestyret delegerer til kontrollutvalget å gjøre endring i planene.

B: Kommunestyrets vedtak:

Utvalgsmøte

PS 71/24 Plan for forvaltningsrevisjon og eierskapskontroll

Kontrollutvalgets innstilling:

Kommunestyret slutter seg til kontrollutvalgets forslag til plan for forvaltningsrevisjon og eierskapskontroll i valgperioden.

Kommunestyret delegerer til kontrollutvalget å gjøre endring i planene.

Saksprotokoll i Kommunestyret - 23.10.2024 - 71/2024 :

Behandling:

Enstemmig vedtak:

Kontrollutvalgets innstilling ble enstemmig vedtatt.

Vedtak:

Kommunestyret slutter seg til kontrollutvalgets forslag til plan for forvaltningsrevisjon og eierskapskontroll i valgperioden.
Kommunestyret delegerer til kontrollutvalget å gjøre endring i planene.

Appendiks 2 – Lenker til lover/regler og tilsynsmyndigheter

Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven) - Lovdata

Forskrift om kommunal beredskapsplikt - Lovdata

Datatilsynet - personvern og informasjonssikkerhet | Datatilsynet

Kommunal beredskap | Statsforvalteren i Nordland

Statsforvalterne-tilsynskalender

Statlige tilsynsetater som fører tilsyn gjennom Statsforvalteren
Utdanningsdirektoratet
Integrerings- og mangfoldsdirektoratet
Direktoratet for samfunnssikkerhet og beredskap
Miljødirektoratet
Statens helsetilsyn

Statlige tilsynsetater som fører tilsyn direkte med kommuner og fylkeskommuner
Arbeidstilsynet
Mattilsynet
Datatilsynet
Arkivverket
Kystverket
Direktoratet for samfunnsikkerhet og beredskap
Kartverket

RM Revisjon Midt-Norge

Informasjonssikkerhet

Brønnøy kommune

Prosjektplan forvaltningsrevisjon

FR1320

2024

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å undersøke om kommunen sitt arbeid med informasjonssikkerhet og personvern er i tråd med regelverk og anerkjente standarder.

PROBLEMSTILLINGER

1. Har kommunen etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket?
2. Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet og personvern?

TIDS- OG RESSURSBRUK

Timeforbruk: 250 timer

Rapport til sekretær: 15.11.2025

OPPDRAGSANSVARLIG REVISOR

Margrete Haugum
mha@revisjonmidtnorge.no

Tlf. 952 33 007

2 MANDAT

I dette kapitlet redegjøres det for bakgrunnen for utkast til prosjektplan.

2.1 Bestilling

Basert på plan for forvaltningsrevisjon har sekretær for kontrollutvalget bedt om å få tilsendt et prosjektutviklingsnotat som grunnlag for bestilling av en forvaltningsrevisjon om informasjonssikkerhet og personvern. Revisjon Midt-Norge har de siste årene gjennomført flere forvaltningsrevisjoner med dette teamet, eksempelvis i Bodø kommune på oppdrag fra Salten kommunerevisjon og i Melhus kommune. Basert på erfaringene fra gjennomførte forvaltningsrevisjonsprosjekter legger revisor i samråd med sekretær fram et forslag til prosjektplan som grunnlag for kontrollutvalgets bestilling.

Kommunene Brønnøy, Vega, Bindal, Sømna og Vevelstad har sammen dannet det kommunale oppgavefellesskapet Kystriket IKT, hvor Brønnøy kommune er kontorkommune. Kystriket IKT sitt formål er å samarbeide om IKT-tjenester for at den enkelte deltaker skal få utført sine lovpålagte oppgaver og andre offentlige oppgaver på en kostnadseffektiv og sikker måte. Kystriket IKT har ansvar for driftsplattformen som understøtter IKT-tjenestene i deltakerkommunene. Kommunene har gjort en felles anskaffelse av driftsleverandør som ekstern samarbeidspart for det kommunale oppgavefellesskapet.

Slik revisor har forstått det er forvaltningsrevisjonen aktuell for kommunene Brønnøy, Bindal, Sømna og Vega. Forvaltningsrevisjonene for dette temaet bør ses i sammenheng ettersom kommunene har et utstrakt samarbeid på området.

2.2 Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å beskytte informasjonsverdier mot skade eller tap. En informasjonsverdi kan være selve informasjonen, men også ressurser for representering og behandling av informasjonen. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser (Jøsang 2021). Videre skriver Jøsang (2021) at det ikke er noen tydelig avgrensning av hva som kan være informasjonsverdi. Derimot er det en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på konfidensialitet, integritet og tilgjengelighet.

Informasjonssikkerhet omfatter:

- konfidensialitet (sikre at informasjonen ikke blir kjent for uvedkommende)
- integritet (sikre at informasjonen ikke blir endret utilsiktet av uvedkommende)

- tilgjengelighet (sikre at informasjonen er tilgjengelig ved behov).

Informasjonssikkerhet handler om hvordan en organisasjon sikrer informasjon og tjenester, og hvilke rutiner og prosesser den bruker. Sentralt her er sikkerhetsledelse og risikostyring. En god sikkerhetskultur er viktig, siden angrep kan forekomme i hele virksomheten, ikke bare på grunn av tekniske sårbarheter. I forvaltningsrevisjonen vil begrepet informasjonssikkerhet og IKT-sikkerhet (informasjons- og kommunikasjonsteknologi sikkerhet) brukes om hverandre.

Det er minst tre juridiske tilnærmeringer til sikkerhetsarbeidet. Disse er:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften), § 15 om internkontroll på informasjonssikkerhetsområdet.

Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem, som samordnes med virksomhetens styrings-system. Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal be-handles. I eForvaltningsforskriften er internkontroll på informasjonssikkerhetsområdet regulert. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikker-hetsområdet som bør være integrert som en del av virksomhetens helhetlige styringssystem.

Personopplysningsloven er bygget på noen grunnleggende personvernprinsipper, og alle som behandler personopplysninger må følge disse prinsippene. Datatilsynet skriver at prinsippene gir uttrykk for at behandling av personopplysninger skal skje på en måte som sikrer forutsigbarhet og forholdsmessighet for enkeltmenneske[1]. Tabellen nedenfor er basert på Datatilsynet sin gjennomgang av personvernprinsippene.

[1] Personvernprinsippene | Datatilsynet

Tabell 1. Personvernprinsippene

Prinsipp	Nærmere om prinsippene
Lovlig, rettferdig og gjennomsiktighet	Rettslig grunnlag for en planlagt behandling av personopplysninger. Behandlingen av personopplysninger skal være gjennomsiktig. Virksomhetene har en behandlingsansvarlig som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Formålsbegrensing	Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist.
Dataminimering	Begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet.
Riktighet	Korrekte opplysninger og skal oppdateres om nødvendig.
Lagringsbegrensning	Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.
Integritet og konfidensialitet	Behandlingsansvarlig må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger.
Ansvarlighet	Punktet understreker ansvaret for å opptre i henhold til regelverket. Virksomhetene må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen. Virksomheten må opptre proaktiv og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Kilde: Datatilsynet

Norge har et eget ekspertorgan for informasjons- og objektsikkerhet, Nasjonal sikkerhets-myndighet (NSM), som er det nasjonale fagmiljøet for IKT-sikkerhet. NSM har utarbeidet en veileder i sikkerhetsstyring[2]. Veilederen beskriver sikkerhetsstyring som systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd:

Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

Utgangspunktet for sikkerhetsstyringen er risikovurderinger som omfatter informasjon om verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene danner grunnlaget for risikohåndteringen. Risikohåndtering omfatter etablering av sikkerhetstiltak, tilpasset de skjermingsverdige verdiene en virksomhet forvalter. Sikkerhetstiltak kan være både organisatoriske tiltak og tekniske tiltak. Organisatoriske tiltak er for eksempel roller og ansvar, kompetanse, retningslinjer, prosedyrer og rutiner. Tekniske tiltak er eksempelvis IKT-løsninger, brannmurer, skap, dører, rom og bygninger.

Figuren nedenfor illustrere sammenhengen i det som er beskrevet ovenfor.

[2] veileder-i-sikkerhetsstyring.pdf

Figur 1. Sammenhenger for sikkerhetsstyring.

NSM har også utarbeidet grunnprinsipper for IKT-sikkerhet[3] (NSM 2020) som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på organisatoriske og teknologiske tiltak. Grunnprinsippene er inndelt i fire kategorier og er gjengitt i tabellen nedenfor.

Tabell 2. Grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende systemer Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontrollere dataflyt Ha kontroll på identiteter og tilganger Beskytte data i ro og i transitt Beskytte e-post og nettleser Etablere evne til gjenoppretting av data Integrere sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengingstester	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Kilde: Nasjonal sikkerhetsmyndighet 2020

[3] Introduksjon - Nasjonal sikkerhetsmyndighet

Organisering av tjenestene

Kommunene Brønnøy, Bindal, Sømna og Vega er revisjonsobjekt. Kommunene samarbeider innenfor IKT-området i det kommunale oppgavefellesskapet Kystriket IKT. Kystriket IKT er derfor sentral i revisjonen. Kommunene har inngått en avtale med en driftsleverandør innenfor IKT som har betydning for hvordan kommunene arbeider med informasjonssikkerhet og personvern.

3 PROSJEKTDESIGN

Kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

I dette utkastet til felles prosjektplan er det utarbeidet to problemstillinger som skal besvares i prosjektet.

1. Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
2. Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Den første problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet. Risikovurderinger og risikohåndtering er sentralt her. Problemstillingen ser på om kommunen har vurdert hvilke informasjonsverdier kommunen har, hvilke trusler som finnes og hvor sårbar kommunen er hvis denne informasjonen ikke blir tilgjengelig eller kommer på avveie. Revisor vil se på om informasjonssikkerhet er en del av kommunens internkontrollsystem, uten at det er en revisjon av internkontrollen i kommunen. En del av problemstillingen er å se om kommunen ivaretar personopplysninger i tråd med krav i regelverket. Eksempelvis om kommunen har full oversikt over sin behandling av personopplysninger og om kommunen har etablert tiltak som sikrer at regelverket følges. Kommunen har blant annet plikt til å føre protokoller over behandlingsaktivitetene de gjennomfører.

Den andre problemstillingen handler om konkrete organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Rammene for problemstillingene er Nasjonal sikkerhets-myndighets grunnprinsipper for IKT-sikkerhet, jfr. tabell 2. Nedenfor er de fire prinsippene listet opp og det er gitt eksempler på hva som er relevant å undersøke på de fire områdene. Listen er ikke uttømmende. Revisor vil også vurdere å benytte ISO 27001 om ledelsessystemer for informasjonssikkerhet.

- Identifisere og kartlegge
    - Om kommunen har oversikt over enheter i IKT-systemet og programvare.
    - Om kommunen har oversikt over brukere av systemet.
- Beskytte og opprettholde
    - Om kommunen har etablert og dokumentert en sikker IKT-arkitektur.
    - Om kommunen har styring med sikkerhetsoppdateringer og en plan for sikkerhetskopieringer og om de tar sikkerhetskopier.

- Oppdage
    - Om kommunen har et system for å overvåke sikkerheten og analysere data fra overvåkningen.
    - Om kommunen gjennomfører inntrengningstester.
- Håndtere og gjenopprette
    - Om kommunen har en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon og loggføring) og en plan for gjenoppretting.

3.2 Avgrensing

Personopplysningsloven stiller krav til behandling av personopplysninger. Revisjonen har ikke kapasitet til å gå i dybden på alle de spesifikke kravene som omhandler behandling av personopplysninger, men vil ha oppmerksomheten rettet mot systemet for behandling av personopplysninger. Revisjonen vil ikke se på behandlingsgrunnlaget som ligger til grunn for behandling av hver enkelt personopplysning til hvert enkelt formål, for eksempel om det er innhentet samtykke.

På området informasjonssikkerhet finnes det mest sannsynlig gradert informasjon. Revisor vil undersøke dette så langt som mulig, men det er begrensede muligheter for å omtale hva som finnes av hensyn til sikkerheten.

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- Lov om kommuner og fylkeskommuner kapittel 25 (kommuneloven)
- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- ISO 27001
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

3.3.1 Mulige revisjonskriterier

Revisjon Midt-Norge har de siste årene gjennomført flere forvaltningsrevisjoner innenfor informasjonssikkerhet og personvern. Dette gir oss et grunnlag for å bygge videre på kunnskap

fra disse revisjonene, og muligheten til å ta utgangspunkt i revisjonskriterier som vi har erfart fungerer god for å belyse problemstillingene.

Problemstilling: *Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?*

- Kommunen skal ha et styringssystem for sikkerhet som omfatter informasjons-sikkerhet, som angir
  - Sikkerhetsmål
  - Sikkerhetsstrategi
  - Sikkerhetsorganisasjon, hvor roller og ansvar framgår
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- Kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.
- Kommunen må ha et avvikssystem og ansatte må melde avvik.
- Kommunen bør evaluere og lære av hendelser.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Problemstilling: *Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?*

Identifisere og kartlegge

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

Beskytte og opprettholde

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- Kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Oppdage

- Kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.
- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Håndtere og gjenopprette

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

3.4 Metoder for innsamling av data

Revisor vil innhente dokumentasjon fra kommunen for å besvare problemstillingene. Gjennomgang av kommunale dokumenter vil være en viktig datakilde for å undersøke hvordan kommunen jobber med informasjonssikkerhet. Eksempler på dokumenter er risikovurderinger, beredskapsplaner, politiske dokumenter som gir føringer, rutinebeskrivelser for ulike tiltak og ulike planer innenfor informasjonssikkerhet, dokumentasjon av behandling av person-opplysninger med mer. Driftsavtalen med driftsleverandøren vil være et sentralt dokument for revisor. Dokumentgjennomgang er en god metode for å finne frem til opplysninger som er nødvendige og relevante for kommunal oppgaveløsning og forvaltning. Det offentlige har i enkelte tilfeller plikt til å dokumentere sitt arbeid og sin regeletterlevelse. Informasjonssikkerhet og personvern er underlagt internkontroll og er relevant å se på meldte avvik på dette området.

Det vil bli gjennomført intervjuer med kommunens ledelse og de som arbeider innenfor det kommunale oppgavefellesskapet, for å få dybdekunnskap om hvordan arbeidet med informasjonssikkerhet foregår i kommunen og for å forstå sammenhengene. Intervjuene kan gi informasjon om at det som er beskrevet i dokumentasjonen fungerer i praksis. Det kan også være aktuelt å intervjue personvernombudet i kommunen og andre ansatte i kommunen.

Forvaltningsrevisjoner på området informasjonssikkerhet og personvern vil kunne komme i berøring med informasjon om sikkerhetsmessige forhold som ikke bør offentliggjøres. Det betyr at ikke alle detaljer i slike forvaltningsrevisjoner kan legges fram i en rapport.

Revisor vil underveis vurdere å gjennomføre en kort elektronisk spørreundersøkelse til ansatte i kommunen, hvis dette lar seg gjøre på en enkel måte. Hensikten er å kartlegge bevisstheten om og opplæring i informasjonssikkerhet. Erfaringer fra tidligere revisjoner er at mange peker på at brukerne er den største sikkerhetstrusselen.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig forvaltningsrevisor	Margrete Haugum
Prosjektmedarbeider	Anna Ølnes
Kvalitetssikrer	Hanne Marit Ulseth Bjerkan
Kvalitetssikrer	Anne Grete Wold

Prosjektteamet vil håndtere alle fire forvaltningsrevisjonene. Alle får oppdragsansvar for en kommune, er medarbeider for en kommune og kvalitetssikrer for to kommuner.

4.2 Milepælsplan

Bestillingsdato	
Prosjektplan til sekretær	Utkast 14.11.2024
Oppstartsmøte	Innen 01.05.2025
Datainnsamling ferdig	30.08.25
Rapport til uttalelse	15.10.25
Rapport til sekretær	15.11.25

Steinkjer 18.11.2024

Oppdragsansvarlig revisor

Margrete Haugum

KILDER

Lov om nasjonal sikkerhet (Sikkerhetsloven)

Lov om behandling av personopplysninger (Personopplysningsloven)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

«Veileder i sikkerhetsstyring», Nasjonal sikkerhetsmyndighet

«NSMs Grunnprinsipper for IKT-sikkerhet», Nasjonal sikkerhetsmyndighet

Datatilsynet – personvernprinsippene

Jøsang, A. (2021) Informasjonssikkerhet. Teori og praksis. Universitetsforlaget, Oslo

ISO 27001 Ledelsessystemer for informasjonssikkerhet

Kommunens hjemmeside

Vurdering av uavhengighet.
Revisors egenvurdering i forbindelse med forvaltningsrevisjonsprosjekt:

Prosjektnr: FR1320	**Kommune: Brønnøy**

Hovedreferanse:
Kommuneloven § 24-4
Forskrift om kontrollutvalg og revisjon kapittel 3
RS 200 --- Formål og generelle prinsipper for revisjon av regnskaper pkt. 4
RS 220 -- Vilkår for revisjonsoppdrag pkt. 4, 12-13
RS 300 -- Planlegging av revisjon av regnskaper pkt. 6
Standard for forvaltningsrevisjon RSK 001 pkt. 8

Ansettelsesforhold:	Undertegnede har ikke ansettelsesforhold i andre stillinger enn Revisjon Midt-Norge SA
Medlem i styrende organer	Undertegnede er ikke medlem av styrende organ i noen virksomhet som ovenfor nevnte kommune deltar i.
Delta eller inneha funksjoner i annen virksomhet, som kan føre til interessekonflikt eller svekket tillit	Undertegnede deltar ikke i eller innehar funksjoner i annen virksomhet som kan føre til interessekonflikt eller svekket tillit til rollen som revisor.
Nærstående	Undertegnede har ikke nærstående som har tilknytning til ovenfor nevnte kommune som har betydning for uavhengighet og objektivitet.
Rådgivnings- eller andre tjenester som er egnet til å påvirke revisors habilitet	Før slike tjenester utføres foretas en vurdering av rådgivningens eller tjenestens art i forhold til revisors uavhengighet og objektivitet. Dersom vurderingen konkluderer med at utøvelse av slik tjeneste kommer i konflikt med bestemmelsen i forskriften § 18, skal revisor ikke utføre tjenesten. Hvert enkelt tilfelle må vurderes særskilt. Revisor besvarer løpende spørsmål/henvendelser som er å betrakte som veiledning og bistand og ikke revisjon. Paragrafen sier at også slike veiledninger må skje med varsomhet og på en måte som ikke binder opp revisors senere revisjons- og kontrollvurderinger. Undertegnede har ikke ytet rådgivnings- eller andre tjenester overfor ovenfor nevnte kommune som kommer i konflikt med denne bestemmelsen.
Tjenesten under kommunens egne ledelses- og kontrolloppgaver	Undertegnede har ikke ytet tjenester overfor ovenfor nevnte kommune som hører inn under kommunens egne ledelses- og kontrolloppgaver.
Opptre som fullmektig for den revisjonspliktige	Undertegnede opptrer ikke som fullmektig for ovenfor nevnte kommune.
Andre særegne forhold	Undertegnede kjenner ikke til andre særegne forhold som er egnet til å svekke tilliten til uavhengighet og objektivitet.

Sted: Steinkjer Dato: 18.11.24
Rolle: Oppdragsansvarlig forvaltningsrevisor
Navn: Margrete Haugum Margrete Haugum

Revisjon Midt-Norge SA
Brugata 2
7716 Steinkjer
post@revisjonmidtnorge.no
907 30 300
www.revisjonmidtnorge.no
Kontonummer: 4270.18.38658
Org.nr: 919 90 2310 MVA

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no