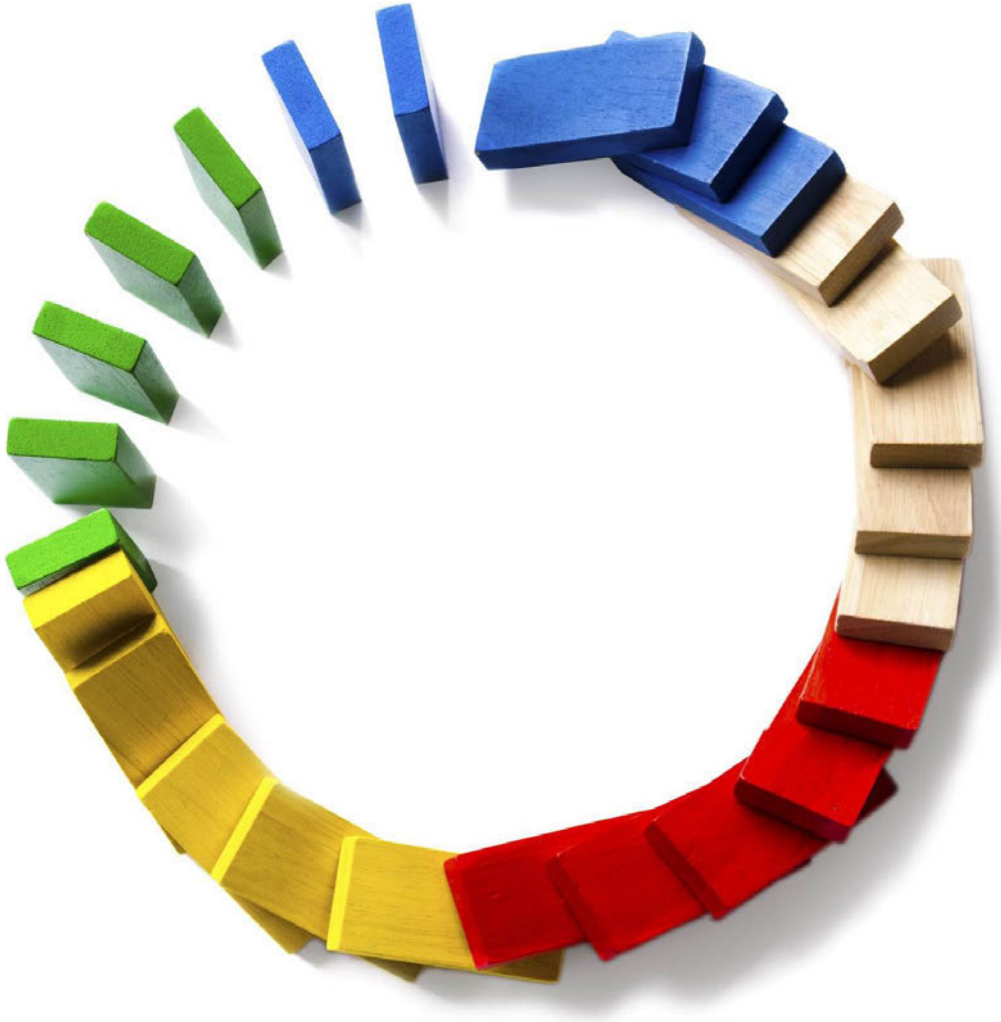
Deloitte.



Forvaltningsrevisjon | Rana kommune

Samfunnssikkerhet og beredskap

Mai 2026

«Forvaltningsrevisjon av
samfunnssikkerhet og beredskap»

Mai 2026

Rapporten er utarbeidet for Rana
kommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen, 5892
Bergen
tlf: 55 21 81 00
www.deloitte.no
forvaltningsrevisjon@deloitte.no

Sammendrag

Deloitte har gjennomført en forvaltningsrevisjon av samfunnssikkerhet og beredskap i Rana kommune. Prosjektet ble bestilt av kontrollutvalget i Rana kommune 23.10.2025 i sak 49/25. Formålet med forvaltningsrevisjonen har vært å undersøke om Rana kommune har etablert tilstrekkelige systemer og rutiner for å sikre at kommunen er godt nok forberedt på å håndtere uønskede hendelser og krisesituasjoner, på en måte som ikke truer vesentlige verdier eller setter innbyggernes liv og helse i fare. I forvaltningsrevisjonen er det gjennomført dokumentanalyse av planer og rutiner, og intervju med ledere og ansatte. Oppdraget er gjennomført i tidsrommet november 2025 til april 2026.

Overordnet beredskap

Undersøkelsen viser at Rana kommune har definert roller og ansvar i beredskapsorganiseringen i tråd med forskrift om kommunal beredskapsplikt § 4. Både kommunal kriseledelse (KKL) og beredskapsstabenes roller og ansvar fremstår godt dokumentert.

Det er etablert kriterier for når kommunal kriseledelse (KKL) skal settes, og når hendelser skal håndteres på sektornivå. Kommunen legger opp til at det i hovedsak skal settes krisestab på sektornivå, noe Deloitte mener er i samsvar med nærhetsprinsippet og ansvarsprinsippet. Samtidig har KKL en viktig funksjon ved hendelser som går på tvers av sektorene, og det er i planverket fastsatt kriterier for når KKL skal etableres. Deloitte stiller spørsmål ved om KKL i praksis settes i henhold til de fastsatte kriteriene, ettersom erfaringer fra tidligere hendelser kan tyde på at terskelen for å etablere KKL har vært høyere enn kriteriene legger opp til.

Det er samtidig noe uklart når og hvordan sentral beredskapskoordinator skal involveres i håndteringen av hendelser i sektorene, herunder hvordan vedkommende skal involveres for å sikre at koordinators kompetanse og helhetsperspektiv bringes inn i sektorarbeidet. Hverken sentral eller sektorenes beredskapskoordinatorer er omtalt i overordnet beredskapsplan, og Deloitte anbefaler at dette tydeliggjøres i planverket.

Kommunen har gjennomført og dokumentert en helhetlig risiko- og sårbarhetsanalyse i tråd med kravene i sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt. Analysen er forankret i kommunestyret, utarbeidet etter DSBs veileder og identifiserer 11 uønskede hendelser med vurderinger av sannsynlighet, sårbarhet og konsekvenser. Deloitte merker seg at ikke alle risikoreduserende tiltak knyttet til helhetlig ROS er fulgt opp innen fastsatte frister.

Kommunen har etablert et overordnet beredskapsplanverk som i hovedsak oppfyller kravene i sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt § 4. Det er utarbeidet beredskapsplaner på tre nivåer som inneholder de påkrevde elementene, herunder plan for kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for krisekommunikasjon. Deloitte merker seg likevel at kommunen ikke har utarbeidet en samlet oversikt over hvilke enhets- og delplaner som foreligger på tvers av virksomhetene. DSB anbefaler at en slik oversikt inngår i beredskapsplanen. Undersøkelsen viser også at flere av beredskapsplanene ikke er revidert i samsvar med kommunens egne frister. Deloitte vil særlig

påpeke at sektorplan for oppvekst ikke er revidert siden 2017. Deloitte mener dette er uheldig og svekker kommunens beredskap knyttet til dette tjenesteområdet.

Deloitte vurderer at kommunens tilnærming – der sektorer håndterer hendelser i eget ansvarsområde og KKL settes ved tverrsektoriell samhandling – er i samsvar med ansvarsprinsippet og likhetsprinsippet, samt DSBs anbefaling om en generisk tilnærming («*all hazard approach*») i overordnet beredskapsplan. Undersøkelsen viser samtidig at overordnet beredskapsplan ikke omtaler de øvrige beredskapsplanene i kommunen eller sammenhengen mellom dem. Etter Deloittes vurdering svekker dette planens funksjon som samordnende dokument, jf. forskrift om kommunal beredskapsplikt § 4 og DSBs veileder, som forutsetter at overordnet beredskapsplan samordner og integrerer andre beredskapsplaner og gir en struktur som viser sammenhengen mellom det overordnede planverket og beredskapsplaner innenfor ulike fagområder.

Kapasiteten til å håndtere alvorlige hendelser opplyses å være tilstrekkelig, og kommunen har vist evne til å håndtere reelle hendelser i linjeorganisasjonen. Kommunen har etablert et rammeverk for opplæring med kompetansekrav og øvelsesfrekvens, og det er gjennomført flere øvelser i perioden 2023–2025 med relevante scenarioer. Det er videre etablert rutiner for evaluering av øvelser og hendelser. Kapasiteten til det forebyggende beredskapsarbeidet vurderes samtidig ulikt internt. Opplæring er ikke dokumentert på en måte som gjør det mulig å ettergå om alle med roller i krisehåndteringen har fått nødvendig opplæring. Øvingsplanen er heller ikke fulgt på overordnet nivå, og ikke alle sektorer har ferdigstilt egne øvingsplaner. Videre viser statusoversikten at i overkant av en tredjedel av tiltakene etter EKOM-hendelsene ikke er påbegynt, selv om fristene er passert, noe som kan indikere at kapasiteten i beredskapsarbeidet ikke er tilstrekkelig.

Kommunen har etablert flere gode arenaer for samarbeid og samhandling, og eksternt samarbeid med blålysetater, frivillige organisasjoner og interkommunale aktører vurderes som godt. Intern samhandling har ved flere faktiske hendelser fungert godt. EKOM-hendelsene i desember 2025 avdekket samtidig svakheter i samhandlingen mellom sektorer, og kommunal kriseledelse ble ikke satt under hendelsene, til tross for at flere av planverkets egne kriterier for dette fremstod som oppfylt. Beredskapsrådet har ikke vært operativt over en lengre periode, noe som ikke er i samsvar med DSB sin veileder til forskrift om kommunal beredskapsplikt eller kommunens eget vedtak. Deloitte merker seg at det er tatt initiativ til reetablering.

Håndtering av cyberangrep

Kommunen har etablert en sikkerhetsorganisasjon med dedikerte roller og faste møtestrukturer for IKT-sikkerhet, med tverrsektoriell samordning gjennom sikkerhetsgruppen og CIKTSO-gruppen. I undersøkelsen pekes det samtidig på at sikkerhetsorganisasjonen har flere sårbare roller, ettersom vesentlig kompetanse konsentrert hos få personer, noe som gjør arbeidet med IKT-sikkerhet personavhengig.

Kommunen har gjennomført en egen IKT-ROS strukturert etter NSMs grunnprinsipper, som er koblet til kommunens helhetlige ROS. Dette bidrar til at IKT-sikkerhetsrisiko ses i sammenheng med kommunens øvrige risikobilde. Det foreligger samtidig ikke en oppdatert ROS-analyse eller DPIA for det forretningskritiske systemet Profil omsorg, og det er dokumentert et vedvarende etterslep av ROS- og DPIA-vurderinger ved anskaffelse av nye IKT-systemer.

Kommunen oppfyller i hovedsak kravet om en overordnet beredskapsplan som integrerer planer for håndtering av digitale hendelser. Det foreligger imidlertid ikke et dedikert tiltakskort tilpasset bortfall av Profil omsorg, og beredskapsplanverket adresserer i begrenset grad sammenhengen mellom IKT-avdelingens planer og fagmiljøenes behov. Ansatte i virksomhetene med system- og beredskapsansvar for forretningskritiske systemer mangler innsikt i overordnede ROS-analyser og cyberangrepsscenarioer. Etter Deloittes vurdering innebærer også plasseringen av det operative cyberangrepsplanverket primært på avdelingsnivå en risiko for at alvorlige digitale hendelser ikke i tilstrekkelig grad forankres og koordineres på overordnet ledelsesnivå.

Kommunen har etablert gode samarbeidsformer med relevante eksterne aktører, herunder KommuneCERT og Helse-CERT. Casegjennomgangen av Profil omsorg viser samtidig utfordringer i samhandlingen på operativt nivå, med uklare ansvarsforhold mellom IKT-avdelingen og driftsleverandøren. Dette har resultert i at det i enkelte saker har tatt lengre tid for systemansvarlig å få nødvendig bistand.

Kommunen har iverksatt hensiktsmessige internkontrolltiltak på flere sentrale områder, særlig knyttet til autentisering, sikkerhetskopiering og overvåking. Samtidig er ikke alle retningslinjer og rutiner fullt ut implementert og etterlevd, og kommunen bør jobbe videre med å styrke opplæringstiltak blant ansatte. Kommunen har etablert en praksis for evaluering av gjennomførte øvelser og tiltak på IKT-sikkerhetsområdet, herunder evaluering av skrivebordsøvelser og opplæringstiltak som del av ledelsens gjennomgang.

Casegjennomgangen av Profil omsorg viser at kommunen har iverksatt relevante sikkerhetstiltak, herunder detaljert tilgangsstyring, tofaktorautentisering og sikkerhetskopiering. Samtidig foreligger det mangler knyttet til systemspesifikk risikovurdering, dedikert tiltakskort for bortfall av systemet, innsikt i overordnede cyberangrepsscenarioer blant ansatte med beredskapsansvar, samt svakheter i samhandlingen mellom fagmiljøet, IKT-avdelingen og driftsleverandøren.

Bortfall av kritisk vei

Sektorberedskapsplanen for teknisk sektor angir overordnede fullmakter, varslingsliste og tiltakskort som fordeler oppgaver mellom avdelingene. Planen beskriver imidlertid ikke hvem som inngår i beredskapsstaben eller deres roller og ansvar, og den nevner ikke hvem som har ansvar for trafikkberedskap på eget veinett (se kommunens plikter som kommunal veimyndighet i vegloven § 10 og veidata- og trafikkinformasjonsforskriften § 14-1).

Kommunen har vurdert risiko for ekstremvær og bortfall av kritisk vei gjennom helhetlig ROS, men det foreligger ikke dokumentasjon av at kommunen har gjennomført risiko- og sårbarhetsanalyser som spesifikt danner grunnlag for trafikkberedskapsplaner og omkjøringsruter for kommunale veier, jf. veidata- og trafikkinformasjonsforskriften § 14-1.

Teknisk sektor har utarbeidet en sektorberedskapsplan med utgangspunkt i helhetlig ROS, og beredskapsplanen inneholder tiltakskort for sektoren på hvert av scenarioene i helhetlig ROS. Tiltakskortene er samtidig ikke inneholder konkrete opplysninger om hvem som har ansvaret og hvordan en slik type hendelse skal håndteres. Kommunen har ikke kategorisert det kommunale veinettet eller utarbeidet trafikkberedskapsplaner, omkjøringsruter eller stengningslenker for kommunale veier, jf. veidata- og trafikkinformasjonsforskriften § 14-1.

Beredskapsplanverket omtaler ikke hvordan kommunen håndterer en situasjon der bortfall av kritisk vei hindrer fremkommeligheten til beboere med behov for helsehjelp.

Det er gjennomført relevante øvelser, men det foreligger ikke en samlet øvingsplan eller formalisert beredskapsopplæring for teknisk sektor som legger opp til systematiske beredskapsøvelser som omfatter ødeleggelse av kritiske veier. Kommunen har etablert rutiner for evaluering av øvelser og hendelser, men evaluering av forbedringspunkter i avdeling drift infrastruktur skjer uten formalisert prosess.

Kommunen har etablert eksternt samarbeid relevant for håndtering av hendelser som fører til ødeleggelse av kritiske veier, men det foreligger ikke dokumentasjon som viser formelt samarbeid med andre veimyndigheter spesifikt om trafikkberedskap, omkjøringsruter og stengningslenker for det kommunale veinettet. EKOM-hendelsene viste at samhandlingen er sårbar når ordinære kommunikasjonskanaler faller bort, noe som er relevant ettersom bortfall av kommunikasjon er en sannsynlig følgehendelse ved ekstremvær.

Anbefalinger

Basert på funn og vurderinger i undersøkelsen anbefaler Deloitte at Rana kommune iverksetter følgende tiltak:

1. Tydeliggjøre beredskapskoordinatorenes roller og mandat i håndteringen av hendelser i overordnet beredskapsplan.
2. Sørge for at kommunen har oppdaterte beredskapsplaner som dekker de mest sårbare risikoområdene.
3. Utarbeide en oversikt over alle beredskapsplanene i kommunen, og vurdere å legge denne inn i overordnet beredskapsplan.
4. Reetablere beredskapsrådet som arena for samordning med eksterne aktører.
5. Sørge for at KKL blir etablert når kriteriene for dette er oppfylt.
6. Sørge for at identifiserte forbedringstiltak blir fulgt opp i samsvar med satte frister.
7. Sørge for at det foreligger oppdaterte risikovurderinger for alle forretningskritiske systemer.
8. Tydeliggjøre roller og ansvar mellom systemansvarlig, IKT-avdelingen og ekstern driftsleverandør.
9. Utarbeide risikovurderinger og kategorisere det kommunale veinettet.
10. Utarbeide trafikkberedskapsplaner for det kommunale veinettet i samråd med øvrige veimyndigheter.
11. Sikre at teknisk sektor sin beredskapsplan definerer krisestabens sammensetning, roller og ansvar.
12. Vurdere å adressere bortfall av kritisk vei i beredskapsplanverket, herunder hvordan fremkommelighet til beboere med behov for helsehjelp skal sikres.

Innhold

Figurer:

Tabeller:

1 Innledning

1.1 Bakgrunn

Deloitte har gjennomført en forvaltningsrevisjon av samfunnssikkerhet og beredskap i Rana kommune. Prosjektet ble bestilt av kontrollutvalget den 23.10.2025 i sak 49/25.

1.2 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å undersøke om Rana kommune har etablert tilstrekkelige systemer og rutiner for å sikre at kommunen er godt nok forberedt på å håndtere uønskede hendelser og krisesituasjoner, på en måte som ikke truer vesentlige verdier eller setter innbyggernes liv og helse i fare.

Med bakgrunn i formålet har følgende problemstillinger blitt undersøkt:

1. **Har kommunen en hensiktsmessig og tydelig overordnet beredskapsorganisering og -planlegging?**
    a) Er roller og ansvar i kommunens beredskapsorganisering tydelig definert, kommunisert og forstått blant alle involverte?
    b) Er helhetlig risiko- og sårbarhetsanalyse gjennomført, dokumentert og oppdatert med tilhørende tiltak?
    c) Foreligger det beredskapsplaner for de mest sårbare risikoområdene, og er disse tilstrekkelig detaljerte, oppdaterte og kjent blant relevante ansatte?
    d) Har kommunen planer som sikrer tilstrekkelig kapasitet og kompetanse i beredskapsarbeidet, og oppdateres disse regelmessig? Under dette:
        i) Er det gjennomført analyser og utarbeidet konkrete tiltak for å sikre tilstrekkelig kompetanse og kapasitet innen beredskapsarbeidet?
        ii) Sikrer kommunen at ansatte i kriseledelsen har tilstrekkelig kompetanse og får nødvendig opplæring, og blir dette jevnlig fulgt opp?
    e) Har kommunen etablert tydelige føringer, rutiner og arenaer for samarbeid og samhandling på tvers av ansvars- og tjenesteområder, og med eksterne aktører, i tråd med samvirkeprinsippet?
    f) Gjennomføres det jevnlige beredskapsøvelser i kommunen? Under dette; har kommunen etablert rutiner for systematisk evaluering og oppfølging av krisehåndtering og planverk etter øvelser og hendelser, slik at forbedringspunkter blir implementert?
2. **Har Rana kommune etablert tilstrekkelig beredskap for håndtering av uønskede digitale hendelser, under dette et cyberangrep mot et utvalgt kritisk system?**
    a) Er roller og ansvar tydelig definert og kommunisert?
    b) Har kommunen gjennomført og dokumentert risiko- og sårbarhetsanalyser som spesifikt omfatter IT-trusler mot et utvalgt kritisk system (som for eksempel

malware, datainnbrudd, tjenestenektangrep (DDoS), og lekkasje av personopplysninger)?

c) Er det utarbeidet beredskapsplaner og tiltakskort som er kjent blant relevante ansatte, og som inneholder konkrete prosedyrer for håndtering av IT-hendelser?

d) Hvordan sikrer kommunen tilstrekkelig samhandling med eksterne aktører, som IT-leverandører og nasjonale sikkerhetsmyndigheter, under håndteringen av et cyberangrep mot et utvalgt kritisk system (jf. samvirkeprinsippet)?

e) Er det iverksatt hensiktsmessige internkontrolltiltak for å redusere risikoen for uønskede digitale hendelser? Under dette tiltak knyttet til:

   i) Innlogging og sikkerhet

   ii) Tilgangsstyring

   iii) Oppdatering og vedlikehold

   iv) Sikkerhetskopi og gjenoppretting

   v) Opplæring av ansatte

   vi) Overvåking og varsling

f) Har kommunen rutiner for å evaluere og forbedre sine digitale beredskapstiltak, basert på erfaringer fra faktiske hendelser eller øvelser relatert til IT-sikkerhet? Under dette; hvordan sikrer kommunen at den er tilstrekkelig oppdatert på nye digitale trusler som dukker opp?

3. Har Rana kommune etablert tilstrekkelig beredskap for håndtering av naturhendelse som fører til ødeleggelse av kritiske veier[1]?

a) Er roller og ansvar tydelig definert og kommunisert?

b) Har kommunen gjennomført og dokumentert risiko- og sårbarhetsanalyser som spesifikt omfatter ødeleggelse av kritiske veier?

c) Foreligger det beredskapsplaner for sykehjem som omtaler ødeleggelse av kritiske veier, og er disse tilstrekkelig detaljerte, oppdaterte og kjent blant relevante ansatte?

d) Har det blitt gjennomført tilstrekkelig opplæring og øvelser for relevant personell som omfatter ødeleggelse av kritiske veier, og involverer disse alle relevante aktører?

e) Har kommunen etablert rutiner for systematisk evaluering og oppfølging av beredskapsplaner etter øvelser og hendelser, og blir forbedringspunkter implementert?

f) Er det utarbeidet tilstrekkelige rutiner og planer for å sikre etterlevelse av samvirkeprinsippet ved ødeleggelse av kritiske veier?

[1] Kritiske veier forstås her som veiforbindelser som er avgjørende for tilgang til og fra viktige samfunnsfunksjoner, som helse- og omsorgsinstitusjoner, nødetater, forsyningslinjer, samt evakuering av innbyggere.

1.3 Metode

Oppdraget er utført i samsvar med gjeldende standard for forvaltningsrevisjon (RSK 001) og kvalitetssikret i samsvar med kravene til kvalitetssikring i Deloitte Policy Manual (DPM).

Oppdraget er gjennomført i tidsrommet november 2025 til april 2026.

1.3.1 Dokumentanalyse

Informasjon om samfunnssikkerhet og beredskap i Rana kommune er samlet inn, og dokumentasjon på etterlevelse av interne rutiner, regelverk mv. har blitt analysert. Innsamlet dokumentasjon har blitt vurdert opp mot revisjonskriteriene. Dokumentanalysen har blitt gjennomført løpende, slik at også dokumenter som har blitt utarbeidet under prosjektperioden har blitt analysert.

1.3.2 Intervju

For å få supplerende informasjon til de skriftlige kildene, har Deloitte intervjuet utvalgte personer i Rana kommune som er involvert i eller har ansvar for beredskap i ulike deler av organisasjonen. Deloitte har intervjuet totalt tolv personer.

1.3.3 Verifiseringsprosesser

Oppsummering av intervju er sendt til de som er intervjuet for verifisering og det er informasjon fra de verifiserte intervjureferatene som er benyttet i rapporten.

Datadelen av rapporten er sendt til kommunedirektøren for verifisering, og tilbakemeldinger er hensyntatt i det videre arbeidet med rapporten. Høringsutkast av rapporten har blitt sendt til kommunedirektøren for uttalelse. Kommunedirektørens høringsuttalelse er lagt ved rapporten i vedlegg 2.

1.4 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteriene er utledet fra autoritative kilder i samsvar med kravene i gjeldende standard for forvaltningsrevisjon. I dette prosjektet er revisjonskriteriene i hovedsak hentet fra sivilbeskyttelsesloven, forskrift om kommunal beredskapsplikt og Nasjonal sikkerhetsmyndighet (NSM) sine prinsipper og anbefalinger knyttet til IT-sikkerhet. Det er også vist til veiloven og forskrift om veidata- og trafikkinformasjon. Kriteriene er nærmere presentert innledningsvis under hvert tema, og i vedlegg 3.

2 Om tjenesteområdet

2.1 Geografiske og demografiske rammer for Rana kommunes beredskapsarbeid

Rana kommune ligger i Nordland fylke og er med sine 4 203 km^2 den største kommunen i fylket målt etter areal. Kommunen hadde per 2025 en befolkning på 25 927 innbyggere, med Mo i Rana som kommunesenter og den nest største byen i Nordland. Kommunen grenser til Sverige i øst, og polarsirkelen går gjennom kommunen. Landskapet er preget av fjell, daler og fjorder, med Ranfjorden som strekker seg inn i kommunen.

Rana kommune er en industrikommune, med tung industri innen metallproduksjon, samt kraft- og vannforsyning. Mo Industripark er blant Norges største industriparker. Kommunen har et stort veinett, med E6 som hovedferdselsåre nordover og sørover, fylkesvei 12 og 17 vestover langs kysten, samt mellomriksveien E12 som forbinder kommunen med Sverige. Mo i Rana har også jernbaneforbindelse og flyplass (Røssvoll).

2.2 Overordnet organisering av kommunens beredskapsarbeid

Rana kommune er administrativt organisert under en kommunedirektør, med fire sektorer: helse og mestring, oppvekst og kultur, teknisk, samt stab og støtte. Hver sektor ledes av en kommunaldirektør. Kommunens beredskapsarbeid er integrert i linjeorganisasjonen, der beredskap er et lederansvar på alle nivåer. Kommunen har en overordnet beredskapskoordinator organisert i sektor for stab og støtte, i tillegg til beredskapskoordinatorer i de øvrige sektorene. Kommunens kriseledelse består av kommunedirektør, ordfører, kommunikasjonssjef, beredskapskoordinator og kommunaldirektørene. Detaljer rundt kommunens organisering av beredskapsarbeidet er nærmere beskrevet i kapittel 3.

2.3 Tidligere undersøkelser av beredskap i Rana kommune

Statsforvalteren i Nordland gjennomførte i 2023 tilsyn med kommunal beredskapsplikt og helseberedskap i Rana kommune. Tilsynet konkluderte med at kommunens arbeid med overordnet beredskap i hovedsak fungerte godt, men påpekte ett avvik knyttet til at kommunen ikke hadde en egen øvingsplan innen helseberedskap. Kommunen opplyser at de hadde en helseberedskapsplan integrert i den overordnede øvingsplanen.

3 Overordnet beredskap

3.1 Problemstilling

I dette kapittelet vil vi svare på følgende hovedproblemstilling og underproblemstillinger:

1. **Har kommunen en hensiktsmessig og tydelig overordnet beredskapsorganisering og -planlegging?**
   a) Er roller og ansvar i kommunens beredskapsorganisering tydelig definert, kommunisert og forstått blant alle involverte?
   b) Er helhetlig risiko- og sårbarhetsanalyse gjennomført, dokumentert og oppdatert med tilhørende tiltak?
   c) Foreligger det beredskapsplaner for de mest sårbare risikoområdene, og er disse tilstrekkelig detaljerte, oppdaterte og kjent blant relevante ansatte?
   d) Har kommunen planer som sikrer tilstrekkelig kapasitet og kompetanse i beredskapsarbeidet, og oppdateres disse regelmessig? Under dette:
      i) Er det gjennomført analyser og utarbeidet konkrete tiltak for å sikre tilstrekkelig kompetanse og kapasitet innen beredskapsarbeidet?
      ii) Sikrer kommunen at ansatte i kriseledelsen har tilstrekkelig kompetanse og får nødvendig opplæring, og blir dette jevnlig fulgt opp?
   e) Har kommunen etablert tydelige føringer, rutiner og arenaer for samarbeid og samhandling på tvers av ansvars- og tjenesteområder, og med eksterne aktører, i tråd med samvirkeprinsippet?
   f) Gjennomføres det jevnlige beredskapsøvelser i kommunen? Under dette; har kommunen etablert rutiner for systematisk evaluering og oppfølging av krisehåndtering og planverk etter øvelser og hendelser, slik at forbedringspunkter blir implementert?

3.2 Revisjonskriterier

Basert på krav i kommuneloven, sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt, har Deloitte utledet følgende revisjonskriterier knyttet til problemstillingen som undersøkes i dette kapitlet:

Tema	Krav kommunen skal ivareta	Kilde til revisjonskriterium
Risiko- og sårbarhetsanalyser	Kartlegge uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse inntreffer, og hvordan de kan påvirke kommunen, og sammenstille dette i en helhetlig risiko- og sårbarhetsanalyse (ROS). ROS skal legge grunnlaget for kommunens arbeid med samfunnssikkerhet og beredskap.	Sivilbeskyttelsesloven § 14; forskrift om kommunal beredskapsplikt § 2

Risiko- og sårbarhetsanalyser	Oppdatere ROS i takt med revisjon av kommunedelplaner og ved endringer i risiko- og sårbarhetsbildet, og forankre den i kommunestyret.	Sivilbeskyttelsesloven § 14; forskrift om kommunal beredskapsplikt §§ 2 og 6
Risiko- og sårbarhetsanalyser; Beredskapsplaner	Utarbeide langsiktige mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhets- og beredskapsarbeidet med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen.	Forskrift om kommunal beredskapsplikt § 3
Roller og ansvar; Beredskapsplaner; Kapasitet og kompetanse; Samhandling og samarbeid	Utarbeide en overordnet beredskapsplan som tydelig angir hvem som utgjør kommunens kriseledelse, samt deres ansvar, roller og fullmakter, inkludert hvem som har myndighet til å bestemme innkalling av kriseledelsen. Planen skal inneholde: • en oppdatert varslingsliste over aktører med roller i krisehåndteringen, • en ressursoversikt som inneholder opplysninger om hvilke ressurser kommunen selv har til rådighet og hvilke ressurser som er tilgjengelige hos andre aktører ved uønskede hendelser, • evakueringsplaner og plan for befolkningsvarsling basert på den helhetlige risiko- og sårbarhetsanalysen, • samt en plan for krisekommunikasjon med befolkningen, media og egne ansatte.	Forskrift om kommunal beredskapsplikt § 4
Beredskapsplaner	Holde beredskapsplanen oppdatert til enhver tid, og som et minimum revidere planen én gang per år. Det skal fremgå av planen hvem som har ansvar for oppdatering, og når planen sist ble oppdatert.	Forskrift om kommunal beredskapsplikt § 6
Samhandling og samarbeid	Etablere samarbeid med andre kommuner om lokale og regionale løsninger av forebyggende og beredskapsmessige oppgaver, med sikte på best mulig utnyttelse av de samlede ressursene, der dette er hensiktsmessig. Kommunen bør etablere et beredskapsråd som arena for samordning og samarbeid, og involvere beredskapsrådet i arbeidet med helhetlig ROS, overordnet beredskapsplan, øvelser og i krisehåndtering.	Forskrift om kommunal beredskapsplikt § 5; Veileder til forskrift om kommunal beredskapsplikt, kapittel 2.3
Kapasitet og kompetanse; Beredskapsøvelser og læring	Kommunen skal ha et system for opplæring som sikrer at ansatte med roller i kommunens krisehåndtering har tilstrekkelige kvalifikasjoner.	Forskrift om kommunal beredskapsplikt § 7
Beredskapsøvelser og læring;	Øve kommunens beredskapsplan minst hvert andre år, med scenario hentet fra kommunens helhetlige risiko- og sårbarhetsanalyse.	Forskrift om kommunal beredskapsplikt § 7

Samhandling og samarbeid	Kommunen skal samarbeide med andre kommuner og relevante aktører i øvelser når scenario og øvelsesform tilsier det.	
Beredskapsøvelser og læring; Risiko- og sårbarhetsanalyser; Beredskapsplaner	Evaluere krisehåndteringen etter gjennomførte øvelser og uønskede hendelser, og gjøre nødvendige endringer i risiko- og sårbarhetsanalysen og beredskapsplanene basert på evalueringene.	Forskrift om kommunal beredskapsplikt § 8
Alle	Ha en systematisk internkontroll, tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren skal: • utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering • ha nødvendige rutiner og prosedyrer • avdekke og følge opp avvik og risiko for avvik • dokumentere internkontrollen i den formen og det omfanget som er nødvendig • evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.	Kommuneloven § 25-1

Se vedlegg 3 for utfyllende revisjonskriterier.

3.3 Datagrunnlag

3.3.1 Roller og ansvar i beredskapsorganiseringen

Kommunens beredskapsplanverk, herunder beskrivelser av roller og ansvar, er dokumentert i kvalitetssystemet EQS. I planverket er det fastslått at kommunen – avhengig av hendelsens art – skal ta hånd om og gi omsorg til skadde og berørte personer og deres pårørende, yte redningstjeneste, helsetjeneste og psykososial omsorg, bistå med evakuering og innkvartering, informere pårørende og media, yte forpleining og forsyningsstøtte (vann, strøm, mat, klær, varme mv.), verne om miljø og materielle verdier, samt stå for opprydding og gjenoppretting. Videre er det fastslått at kommunen under en hendelse skal opprettholde ordinære funksjoner og tjenester, informere befolkningen, media og egne ansatte, sikre tilgang på ressurser og samvirke med frivillige og private aktører. I det følgende gjennomgås roller og ansvar i kommunens beredskapsorganisasjon.

Kommunal kriseledelse og krisestab på sektornivå

Rana kommunes kriseledelse (KKL) er dokumentert i den overordnede beredskapsplanen, administrativt vedtatt av strategisk ledergruppe (SLG) 26. august 2024. Kriseledelsen består av kommunedirektør (administrativ leder), ordfører (politisk leder), kommunikasjonssjef, beredskapskoordinator og alle kommunaldirektørene.[2] Andre fagpersoner som kommuneoverlegen tilkalles ved behov.

Den overordnede beredskapsplanen spesifiserer at kriseledelsen har ansvar for beredskap for sitt fagområde og sine avdelinger, samt operativ ledelse og håndtering av hendelser. Kriseledelsen skal sørge for at det utløses tilstrekkelig ressurser for å

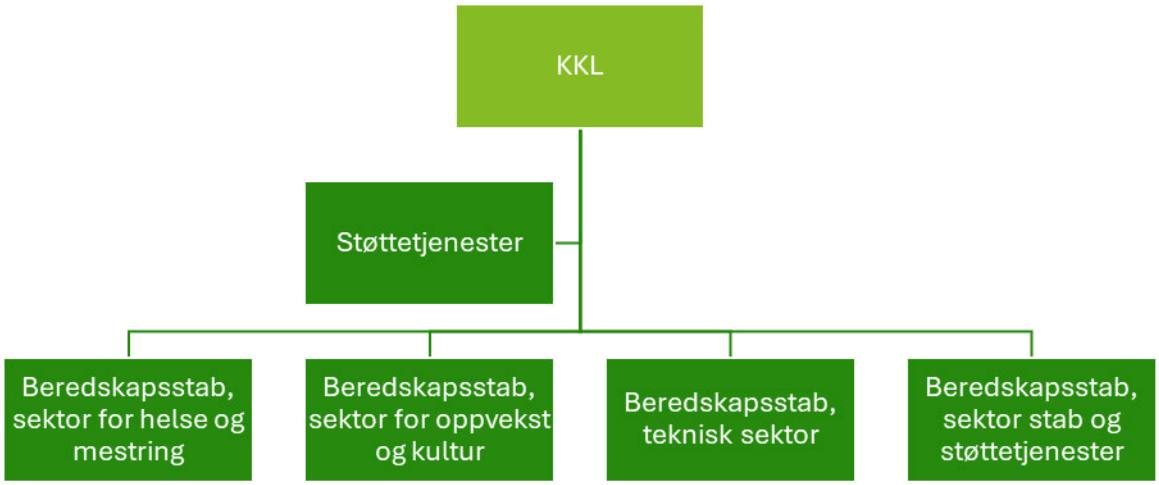
[2] Rana kommune. *Overordnet beredskapsplan Rana kommune*. Plan. Vedtatt SLG 26.08.2024.

iverksette beslutninger, og ha oversikt over ressurser og sårbare områder. Videre skal kriseledelsen etablere et overordnet situasjonsbilde og formidle situasjonsforståelse til aktuelle aktører, raskt beslutte iverksetting av tiltak, og utvikle en strategi for krisehåndtering, herunder planlegging for «worst case». Kriseledelsen har også ansvar for koordinering mellom berørte aktører, krisekommunikasjon internt og eksternt på rett nivå til rett tid, samt ressursprioritering og -fordeling. I tillegg skal kriseledelsen sørge for rapportering til samarbeidsparter, orientering til relevante politiske organ og jevnlig rapportering til Statsforvalteren, samt sikre nødvendige stedfortredere og bemanning. Det fremgår videre at kommunedirektøren er delegert fullmakt til å disponere inntil 1 million kroner i krisesituasjoner. Overskrides dette beløpet, må formannskapet innkalles.

Hver kommunaldirektør har ansvar for beredskapen innenfor sitt fagområde, og skal etablere og lede krisestaben på sektornivå ved hendelser. Kommunaldirektørene er også medlemmer av den sentrale kriseledelsen og rapporterer direkte til kommunedirektøren dersom hendelsen tilsier at sentral kriseledelse settes[3].

Krisestabene på sektornivå har følgende oppgaver, både i rollen som egen krisestab og som støtte til kriseledelsen dersom denne settes: varsle interne og eksterne, overvåke situasjonen og ha dialog med interne og eksterne samfunnssikkerhetsaktører som er berørt av den uønskede hendelsen, samt utvikle og formidle en samlet situasjonsforståelse med utgangspunkt i informasjon fra berørte ansvarsområder i kommunen og andre berørte aktører. Videre skal krisestabene holde kriseledelsen orientert om utviklingen av hendelsen, gi råd til kriseledelsen om mulige tiltak og følge opp besluttede tiltak fra kriseledelsen. Krisestabene skal også ivareta oppgaver knyttet til krisekommunikasjon dersom det ikke etableres egen krisekommunikasjonsstab, samt fungere som en administrativ og praktisk støttefunksjon for kriseledelsen. Krisestabene skal videre sørge for forpleining og hensiktsmessig rullering av personell i kommunens kriseorganisasjon, samt foreta loggføring og situasjonsrapportering etter fastsatte retningslinjer og rutiner ved bruk av krisestøtteverktøyet RAYVN.

Figur 1 – Illustrasjon av organisering av sektorenes beredskapsstaber under KKL



[3] Rana kommune. *Overordnet beredskapsplan Rana kommune*. Plan. Vedtatt SLG 26.08.2024.

Beredskapskoordinatorer og -nettverk

Rana kommune har en **sentral beredskapskoordinator** med ansvar for å koordinere kommunens beredskapsarbeid internt (som bindeledd mellom KKL og sektorene) og eksternt (dialog med statsforvalter, nødetater og nabokommuner), samt ansvar for overordnet beredskapsplanverk. Beredskapskoordinator er medlem av KKL med en rådgivende rolle uten krisefullmakter, og har formelt ansvar for loggføring. En annen rådgiver bidrar med loggføring slik at beredskapskoordinator kan konsentrere seg om rådgivning og samhandling. Beredskapskoordinator har også ansvar for å lede kommunens beredskapsnettverk (omtalt i kapittel 3.3.5).

Det er servicesjef i kommunen som har rollen som beredskapskoordinator. Funksjonen er direkte underlagt kommunaldirektør stab, som ivaretar alle felles administrative støttefunksjoner på vegne av kommunedirektøren etter fullmakt. Servicesjef har til daglig ansvar for blant annet politisk sekretariat, valggjennomføring og sentralbord. Vedkommende har hatt rollen siden 2011 og har mastergrad i samfunnssikkerhet og beredskap. Det er ikke utarbeidet en stillingsinstruks, men rolle og oppgaver er beskrevet i kvalitetssystemet.

I intervju fremkommer det ulike syn på beredskapskoordinators organisatoriske plassering. Fra ett hold beskrives det som et bevisst valg at beredskapskoordinator har linjeansvar i tillegg til beredskapsansvaret, da dette styrker arbeidet gjennom myndighet og etablerte relasjoner. Fra et annet hold vurderes organiseringen som noe fragmentert fordi funksjonen ikke er plassert direkte under kommunedirektøren. Det bemerkes at beredskapskoordinator i beredskapssammenheng rapporterer til kommunaldirektøren for sektor stab og støtte – som opererer på fullmakt fra kommunedirektøren – og dermed er underlagt kommunedirektørnivå i krisesituasjoner, selv om vedkommende i ordinær drift rapporterer til HR- og organisasjonssjefen. Dokumentasjonen viser at dette er tatt opp som et moment i ledelsens gjennomgang for 2025–2026, med anbefaling om å vurdere organiseringen.

I tillegg til den sentrale beredskapskoordinatoren er det utnevnt **beredskapskoordinatorer i sektorene**. Disse er omtalt i sektorplanen for helse og mestring og sektorplanen for beredskap i skoler og barnehager[4], men er ikke nevnt i sektorplanen for tekniske tjenester eller beredskapsplanen for støttetjenester.[5]

Det er ikke utarbeidet stillingsbeskrivelse for sektorenes beredskapskoordinatorer, men nettverkets overordnede funksjon er beskrevet i EQS. Her går det fram at beredskapskoordinatorene skal ivareta sin sektor og bidra i det helhetlige og systematiske beredskapsarbeidet, herunder styrke det forebyggende beredskapsarbeidet, styrke kommunens beredskap og krisehåndteringsevne, sikre internkontroll og arbeide for økt samarbeid og samhandling med andre beredskapsaktører.

[4] Sektorplan: Beredskap for helse- og mestring 2023–2027; Sektorplan for beredskap i skoler og barnehager 2017–2018.
[5] Overordnet beredskapsplan Rana kommune, vedtatt SLG 26.08.2024; Sektorplan beredskap for tekniske tjenester 2024–2027; Beredskapsplan Støttetjenesten 2025–2027

I intervju blir det vist til at rollen som beredskapskoordinator i sektorene innebærer å fungere som bindeledd mellom sentral beredskapsorganisasjon og den enkelte sektor, sikre etterlevelse av lovkrav, gjennomføre opplæring og øvelser, samt støtte loggføring og stabsarbeid via RAYVN. Rollen ivaretas som en del av ordinær stilling. Sektorenes beredskapskoordinatorer møtes i beredskapsnettverket omtrent månedlig for koordinering av planer, systemutvikling og kompetansebygging. I intervju blir det pekt på at det er uklart når og hvordan overordnet beredskapskoordinator skal involveres ved hendelser på lavere nivå, for slik å sikre at kompetansen og helhetsperspektivet inkluderes i sektorens beredskapsarbeid.

Varsling og rapportering

Av overordnet beredskapsplan går det fram at beredskap er et lederansvar, og hendelser skal løses på lavest mulig nivå i tråd med beredskapsprinsippene. Alle ansatte har ansvar for å varsle sin leder ved større uønskede hendelser. Ved større uønskede hendelser skal det også varsles til kommunen sentralt, enten til sentralbord (innenfor normal arbeidstid) eller til medlemmene av KKL ihht. varslingslisten som ligger vedlagt overordnet beredskapsplan (utenfor normal arbeidstid). Beredskapsplanen inneholder kontaktinformasjon til både sentralbordet, og alle medlemmene og varamedlemmene i KKL. Kommunedirektøren har det overordnede ansvaret for å iverksette varsling og etablering av kriseledelsen. Varsling skjer normalt via krisestøtteverktøyet RAYVN, og ved etablering av kriseledelse skal Statsforvalteren i Nordland varsles.

Kommunen har også utarbeidet et operativt støttedokument, «*Hvem kontakter du – beredskap*», som angir hvem ansatte skal kontakte ved ulike typer hendelser.[6] Ved langvarige hendelser skal kriseledelsen sørge for jevnlig orientering til relevante politiske organ og rapportering til Statsforvalteren. Mal for situasjonsrapport finnes i krisestøtteverktøyet og kvalitetsportalen.[7]

I intervju ble det pekt på at den siste større hendelsen, en vinterstorm som førte til bortfall av e-kom[8], illustrerte at operativ ledelse ikke alltid har kapasitet til å loggføre i sanntid i RAYVN under selve krisen. Behovet for bedre støtte til loggføring og tidligere involvering av beredskapskoordinator ble identifisert som læringspunkter i evalueringen etter hendelsen.[9]

Kommunikasjon av roller og ansvar

Av vedlegg 5 til overordnet beredskapsplan fremgår det at linjeleder har ansvar for opplæring av medarbeidere med beredskapsoppgaver, og at opplæringen skal sikre at alle med roller i beredskapsorganisasjonen kjenner til sine roller og ansvar, varslingsrutiner og bruk av krisestøtteverktøyet RAYVN. I intervju blir det pekt på at kommunen i praksis sikrer at ledere og ansatte med roller i kriseledelsen kjenner til sine roller gjennom årlig beredskapsdag, øvelser, kurs og fagdager.

---

[6] Hvem kontakter du – beredskap, ID 8008

[7] Rana kommune. *Vedlegg 3 – Situasjonsrapportering*. Vedlegg til overordnet beredskapsplan. Uten dato.

[8] EKOM (elektronisk kommunikasjon) dekker systemer og tjenester som muliggjør overføring av informasjon via elektriske signaler, samt infrastrukturen som kreves for å støtte kapasitetskrevende tjenester.

[9] Evaluering av EKOM hendelser – 13.–14. desember 2025 og 27.–29. desember 2025 i Rana kommune, 21.01.2026.

I intervju fremkommer det at rolle- og ansvarsforståelsen oppleves som tydelig på toppnivå, der ledere peker på betydelig erfaring fra øvelser og reelle hendelser. Den overordnede beredskapsplanen definerer kriterier for eskalering fra kommunaldirektørnivå og opp til kommunedirektøren, men inneholder ikke tilsvarende formaliserte rutiner for eskalering på lavere nivåer i organisasjonen. I intervju fremkommer det at forståelsen av når og hvordan hendelser skal eskaleres blir mer utydelig lenger ut i organisasjonen, og at dette i stor grad baseres på erfaring og skjønn snarere enn formaliserte rutiner (se kapittel 3.3.4 for mer informasjon om opplæring).

Liaison-funksjonen

Rana kommune har etablert liaison-funksjonen som en del av sin beredskapsorganisering. En liaison er en utpekt person fra Rana kommune som sendes til et annet myndighetsorgan eller en institusjon under håndteringen av en hendelse, med formål om å sikre gjensidig informasjonsutveksling og informasjonsflyt mellom kommunen og den aktuelle virksomheten. Planverket definerer ikke hvem som utpeker eller kan utpekes som liaison, men det fremgår at liaisonen rapporterer til KKL. Liaisonen har ikke beslutningsmyndighet på vegne av Rana kommune, men bistår virksomheten med å finne og etablere kontaktpunkter inn til kommunen. I forbindelse med verifisering opplyser Rana kommune at det er situasjonsavhengig hvem som utpekes som liaison, og at kommunen har etablert rutine og mal for dette. Revisjonen har ikke sett denne.

3.3.2 Risiko- og sårbarhetsanalyser

Helhetlig ROS 2022–2025

Den helhetlige risiko- og sårbarhetsanalysen er dokumentert i rapporten «RanaROS 2022–2025», vedtatt av kommunestyret 10. november 2022 (sak 116/22). Dokumentet inneholder blant annet mål med analysen, kommunens risikobilde presentert i figurer og matriser, metodebeskrivelse, særtrekk og samfunnsmessige forhold i Rana kommune, samt detaljerte analyser av identifiserte scenarioer. Analysegruppen identifiserte 11 scenarioer, herunder ekstremvær og langvarig strømbrudd, kvikkleireskred, pandemi, dambrudd, eksplosjon med påfølgende brann og kjemikalieutslipp, atomulykke, flystyrt, båtulykke, pågående livstruende vold (PLIVO), sikkerhetspolitisk krise med hackeranslag, og utslipp av kjemikalier i drikkevannskilde. Scenarioene danner grunnlaget for kommunens arbeid med beredskapsplanlegging og risikoreduserende tiltak.

For hvert scenario beskrives uønsket hendelse med relevante lokale forhold og mulige årsaker, eksisterende risikoreduserende tiltak, sannsynlighets- og konsekvensvurdering, sårbarhetsvurdering knyttet til kritiske samfunnsfunksjoner, behov for befolkningsvarsling og evakuering, samt forslag til ytterligere risikoreduserende tiltak. ROS-analysen ble sendt på høring i september 2022, og det kom inn høringssvar fra Statsforvalteren i Nordland, Mattilsynet og Statens vegvesen. Innspillene ble tatt hensyn til i den endelige versjonen.[10]

Basert på ROS-analysen utarbeidet kommunen en oppfølgingsplan som spesifiserer 13 overordnede risikoreduserende tiltak med tidsfrister, samt over 100 scenario-spesifikke tiltak fordelt på alle de 11 scenariene. Tiltakene er organisert i kategorier som blant annet

[10] Vedtatt av Kommunestyret 10.11.2022 sak 116/22.

kompetanseheving, planverk, informasjonstiltak, samhandlingstiltak og bygningsmessige tiltak.[11]

I tillegg til den helhetlige ROS-analysen har kommunen utarbeidet flere sektorspesifikke risiko- og sårbarhetsanalyser. Det foreligger en egen ROS-analyse for brann og redning som inneholder vurderinger av 21 uønskede hendelser med tilhørende sårbarhet, sannsynlighet og konsekvenser[12]. Videre er det utarbeidet en overordnet IKT-ROS som vurderer risiko knyttet til kommunens informasjonssystemer og digitale infrastruktur. Kommunedelplan for byutvikling 2024–2034 inneholder også en overordnet ROS-analyse som er relevant for planleggingen av byutvikling i kommunen.

Utarbeidelse av helhetlig ROS

Arbeidet med den helhetlige risiko- og sårbarhetsanalysen ble våren 2022 lagt til en arbeidsgruppe med mandat fra Strategisk Ledergruppe, med tidsplan for ferdigstillelse høsten 2022. Prosjektgruppen bestod av interne deltakere fra ulike sektorer, med prosjektleder fra stab/støtte og representanter fra helse og mestring, oppvekst og kultur, teknisk sektor og kommunikasjon. Prosjektgruppen benyttet DSBs veileder for helhetlig risiko- og sårbarhetsanalyse i kommunene (2014) som metodisk grunnlag, og tok utgangspunkt iblant annet Analyse av krisescenarioer 2019 fra Direktoratet for samfunnssikkerhet og beredskap (DSB), Fylkes-ROS 2019 fra Statsforvalteren i Nordland, samt nasjonale og lokale statistikker og trusselvurderinger.

Eksterne aktører, herunder nødetatene, Sivilforsvaret, Statsforvalteren i Nordland, NVE, Mattilsynet, Helgelandssykehuset, frivillige organisasjoner, nabokommuner, Mo i Rana Havn, Avinor, Statkraft og Mo Industripark, deltok på flere av arbeidsseminarene.

Oppfølging av tiltak i beredskapsarbeidet

I intervju pekes det på at tiltak i beredskapsarbeidet følger samme arbeidsflyt som tiltak i det ordinære arbeidet innen kommunens tjenesteområder. Alle tiltak registreres i kvalitetssystemet EQS, og det gjøres en vurdering av alvorlighetsgrad. Tiltak som haster følges opp umiddelbart gjennom direkte kontakt, mens mindre presserende tiltak følger normal saksgang i kvalitetssystemet. Det blir opplyst om at tiltak som utløser større investeringer og økte driftsutgifter må finansieres, primært gjennom den årlige budsjett- og økonomiplanprosessen, og unntaksvis gjennom ekstraordinære budsjettreguleringer. Som ledd i internkontrollen blir tiltak fulgt opp i den årlige ledelsens gjennomgang, der status gjennomgås og forbedringer foreslås.

Status over beredskapstiltak per november 2025 viser totalt 83 tiltak fordelt på de 11 scenarioene fra den helhetlige risiko- og sårbarhetsanalysen[13]. Oversikten viser navn på tiltak, ansvarlig avdeling og status per 2023, 2024 og 2025. Over halvparten av tiltakene er utført, og mesteparten av de øvrige er påbegynt eller under arbeid. Statusrapporten angir at følgende overordnede tiltak er gjennomført: øvelsesplan, evakueringsplan,

[11] Helhetlig ROS (H-ROS), rutine ID 2381, gyldig fra 03.10.2024.
[12] Risiko- og sårbarhetsanalyse Brann- og ulykkesrisiko, Rana brann og redning og Nesna brannvesen, 17.01.2025
[13] Rana kommune. *Ledelsens gjennomgang - Samfunnssikkerhet og beredskap 2024*. Notat. Behandlet i rådmannens strategiske ledergruppe (SLG) 10. november 2025. Vedlegg: *Status oppfølgingstiltak – beredskap - november 2025 til ledelsens gjennomgang*. Oversikt. 06.11.2025.

atomplan, overordnet beredskapsplan, samlingssteder for informasjon, kjentmenn-ordning, varslingsmaler, krisekommunikasjonsplan, beredskapshotell-avtale, beredskapsdag og kriseportal. Tiltak under arbeid omfatter sektor- og delplanverk, digitale verktøy og kartlegging av ressursoversikter. Tiltak som ikke er påbegynt eller mangler status, inkluderer rutiner for prioriteringsliste kraftforsyning, rutiner for ventilasjon, implementering av veileder for systematisk sikkerhetsarbeid for bygningseier, og rutiner for skjermverdig informasjon. Statusrapporter foreligger for årene 2023, 2024 og 2025.

I intervju vises det til at beredskapskoordinator følger opp og purrer på tiltak som blir liggende urørt over tid, men at det er begrenset kapasitet til denne oppgaven. Oppfølging av tiltak fra den helhetlige ROS har vært utfordrende fordi tiltakene ble identifisert før kvalitetssystemet EQS var på plass, og ble derfor lagt inn i det tidligere systemet CIM. Nå ligger noen tiltak i Word-dokumenter og andre i EQS, noe som har ført til at oppfølging av enkelte tiltak har glippet. I forbindelse med oppdateringen av helhetlig ROS i 2026 planlegges det å legge alle tiltak inn i EQS for bedre systematikk. Det vurderes også å synliggjøre relevant status i Framsikt (system for virksomhetsstyring), med særskilt oppmerksomhet på hva som kan publiseres av hensyn til sikkerhet.[14]

Oppfølging og revidering av helhetlig ROS

Helhetlig ROS 2022–2025 beskriver en overordnet internkontrollprosess for arbeidet med samfunnssikkerhet og beredskap. Overordnet ROS rapporteres til kommunestyret minimum hvert 4. år, oppfølgingsplan rapporteres årlig til Formannskapet, og gjennomførte tiltak rapporteres årlig til Strategisk Ledergruppe gjennom ledelsens gjennomgang. Det er også utarbeidet et årshjul for beredskapsaktiviteter, samt egen rutine for oppdatering av helhetlig ROS-analyse. Rutinen «Helhetlig ROS (H-ROS)» angir at den helhetlige risiko- og sårbarhetsanalysen skal oppdateres i takt med revisjon av kommunedelplaner og ved endringer i risiko- og sårbarhetsbildet, og fullstendig revideres hvert 4. år. Neste revisjon er planlagt i 2026.

I helhetlig ROS går det fram at sektorene skal utarbeide egne risiko- og sårbarhetsanalyser (sektorROS) som grunnlag for sine beredskapsplaner. Helse og omsorg gjennomførte sin sektorROS med oppstart 11. mai 2023, og sektorplanen ble revidert samme år.[15] Oppvekst og kultur har gjennomført sektorROS, men sektorberedskapsplanen er ikke ferdigstilt. Tekniske tjenester har ikke utarbeidet en sektorROS, men har utarbeidet en sektorplan beredskap for tekniske tjenester 2024–2027, basert på den helhetlig ROS i kommunen fra 2022.[16]

3.3.3 Beredskapsplanverk

Oversikt over beredskapsplanverket

Rana kommune har etablert et beredskapsplanverk bestående av tre nivåer. Øverst er overordnet beredskapsplan, som gjelder hele kommunen, og inkluderer 12 vedlegg. Det andre nivået består av sektorberedskapsplanene for de ulike fag- og ansvarsområdene.

[14] Status oppfølgingstiltak – beredskap – november 2025 til ledelsens gjennomgang, 06.11.2025

[15] Rana kommune. *Sektorplan: Beredskap for helse- og mestring 2023 – 2027*. Plan. Vedtatt av kommunestyret 20.05.2014, revidert og administrativt vedtatt 25.01.2023.

[16] Rana kommune. *Sektorplan beredskap for tekniske tjenester 2024-2027 Rana kommune*. Plan. Vedtatt av kommunaldirektør tekniske tjenester 20.9.2024.

Det tredje nivået omfatter enhets- og delplaner for spesifikke virksomheter som skoler, barnehager og sykehjem. Planene skal gjenspeile sektorplanene og være tilpasset den enkelte enhets forhold og ansvar.

Kommunen har ikke utarbeidet en samlet oversikt over hvilke enhets- og delplaner som er utarbeidet på tvers av kommunens virksomheter. Virksomhetene har ansvar for å laste opp sitt planverk i EQS, men undersøkelsen viser at ikke alle planer er lastet opp og at noen ligger lagret i feil mapper i systemet. Tabell 1 gir oversikt over beredskapsplanverket på de ulike nivåene i organisasjonen

Tabell 1: Oversikt over beredskapsplanverket

Nivå	Navn	Beskrivelse	Sist revidert
1	Overordnet beredskapsplan	Gjelder hele kommunen. Inneholder mål og strategier for beredskapsarbeidet, kriterier for etablering av kriseledelse, roller og fullmakter, beredskapsnivåer og 12 operative vedlegg (bl.a. varslingsliste, evakueringsplan, tiltakskort og krisekommunikasjonsplan).	26.08.2024
1	Evakueringsplan	Vedlegg til overordnet plan. Beskriver ansvar, oppgaver og organisering ved evakuering, faser i evakuering, roller for politi, kommune og frivillige, samt oversikt over innkvarteringssteder og samarbeidsaktører.	26.08.2024
1	Atom-beredskapsplan	Vedlegg til overordnet plan. Beskriver beredskapsnivåer, organisering av nasjonal atomberedskapsorganisasjon, kommunens rolle og ansvar, samt ni konkrete tiltak kommunen skal forberede seg på å gjennomføre ved atomhendelser.	05.11.2024
1	Krise-kommunikasjons-plan	Vedlegg til overordnet plan. Inneholder operativ del med umiddelbare tiltak, tiltakskort og kontaktlister for krisekommunikasjon, samt bakgrunn og beskrivelse av prinsipper for kommunikasjon med befolkning, media og egne ansatte.	01.10.2025
1	Beredskapsplan for bemanning	Gjelder alle kommunens virksomhetsområder. Beskriver rammeverk for å sikre nødvendig bemanning i kritiske tjenester ved ekstraordinære forhold, herunder trinnvise tiltak ved bemanningssvikt fra intern omdisponering til ekstern bistand.	10.12.2025
2	Beredskapsplan Støttetjenesten 2025–2027	Gjelder HR- og organisasjonsavdelingen, økonomiavdelingen, IKT-avdelingen og kommuneadvokat. Inneholder roller og ansvar i beredskapsorganiseringen, varslingslister, tiltakskort for 11 hendelser i henhold til RanaROS, samt nødplakat for digitale angrep.	15.10.2025
2	Sektorplan beredskap for helse og mestring 2023–2027	Gjelder sektor helse og mestring. Inneholder sektorens beredskapsorganisering, varslingslister, tiltakskort for hendelser fra RanaROS, kontinuitetsplaner for fagavdelingene, øvingsplan og oversikt over evakueringssteder for helseinstitusjoner og omsorgsboliger.	25.01.2023
2	Sektorplan beredskap for	Gjelder avdelingene bydrift, areal og miljø og byggdrift. Inneholder roller, fullmakter, varslingsliste, oversikt over mannskap og materiell, tiltakskort for 11 hendelser fra	20.09.2024

	tekniske tjenester 2024–2027	RanaROS, samt referanser til underliggende planer (brannordning, VA-beredskapsplan, IUA-plan og evakueringsplaner for idrettsanlegg).	
2	Sektorplan for beredskap i skoler og barnehager (oppvekst og kultur) 2017–2018	Planen er utdatert. Rana kommune opplyser om at det arbeides med en ny sektorberedskapsplan for skoler og barnehage, men at denne ikke er ferdigstilt på revisjonstidspunktet.	25.01.2017
3	Beredskapsplan psykososialt kriseteam	Delplan for psykososialt kriseteam (EPS). Teamet mobiliseres ved hendelser der det er behov for psykososial oppfølging av berørte og pårørende.	25.11.2024
3	Plan for evakuerte- og pårørendesenter	Delplan for etablering og drift av evakuerte- og pårørendesenter (EPS) ved hendelser som krever mottak og oppfølging av evakuerte og pårørende.	27.11.2024
3	Beredskapsplan miljørettet helsevern	Delplan for beredskap innen miljørettet helsevern.	15.11.2024
3	Beredskapsplan IKT	Gjelder IKT-avdelingen. Beskriver organisering og gjennomføring av beredskapsarbeidet ved krisesituasjoner, med særlig vekt på å opprettholde kritiske IT-systemer. Inneholder varslingsprosedyrer, tiltakskort for åtte IT-hendelser, prosedyre for håndtering av cyberangrep og ransomware, samt kontinuitetsplan. Nærmere omtalt i kapittel 4.3.3.	10.12.2025
3	Beredskapsplan informasjonskontor	Delplan for informasjonskontoret ved beredskapshendelser.	25.11.2025
3	Kontinuitetsplan serviceavdelingen	Kontinuitetsplan for serviceavdelingen ved beredskapshendelser.	25.11.2025
3	Plan for brann og redning	Gjelder Rana brann og redning. Samordner oppdaterte ROS-er, beredskapsvurderinger og forebyggende strategier, og utgjør grunnlag for en handlingsplan for brann- og redningstjenesten.	18.11.2025

Rana kommune opplyser at følgende beredskapsplaner er under utarbeidelse:

- Nav beredskapsplan
- Beredskapsplan sentralkjøkken
- Beredskapsplan for sykehjem

Videre opplyser kommunen om at enkelte avdelinger (nivå 3) har utarbeidet kontinuitetsplaner som ikke ligger inne i EQS. Sentral beredskapskoordinator har ikke oversikt over disse planene.

Overordnet beredskapsplan

Den overordnede beredskapsplanen for Rana kommune er delt i en strategisk del og en operativ del.[17] Den strategiske delen inneholder kommunens mål og strategier for beredskapsarbeidet, basert på fire satsingsområder:

- gjennomgående sikkerhetskultur,

[17] Rana kommune. *Overordnet beredskapsplan Rana kommune*. Plan. Vedtatt SLG 26.08.2024.

- tydelig og målrettet krisekommunikasjon,
- systematisk arbeid med å forberede, øve og forbedre, og
- tydelig ivaretakelse av rollen som pådriver og tilrettelegger.

Planen definerer roller og ansvar for kriseledelsen og inneholder to uavhengige mekanismer for håndtering av hendelser. For det første spesifiserer planen seks kriterier for når kommunal kriseledelse bør etableres, herunder hendelser som ikke kan løses gjennom normal drift, som involverer flere sektorer, får store konsekvenser, krever støtte fra eksterne aktører, eller kan medføre stort informasjonsbehov i befolkningen. Det er tilstrekkelig at ett av kriteriene er oppfylt.

For det andre definerer planen tre beredskapsnivåer – grønt, gult og rødt – som gjenspeiler i hvilken grad kommunens tjenester er berørt, fra ubetydelig berørt (ordinær drift) via noen grad berørt (økt aktsomhet og vurdering av lokal stab) til alvorlig berørt (full krisehåndtering der ordinær drift tilsidesettes). Beredskapsnivåene skal benyttes av alle sektorer og er uavhengige av om kommunal kriseledelse er satt; planen åpner for at det kan etableres krisestab på sektornivå uten at kriseledelsen aktiveres, i tråd med nærhetsprinsippet om at kriser skal løses på lavest mulig nivå.

Den operative delen av planen inneholder 13 vedlegg (se tabell 2 for full oversikt), herunder evakueringsplan og varslingsliste. Det fremgår hvordan befolkning og media skal informeres, hvem som har ansvaret for å oppdatere planen, og når den sist ble oppdatert. Beredskapsplanen er skrevet ut i papirform og oppbevares i kriseledelsens møterom samt hos det enkelte medlem av KKL. Det går videre fram av beredskapsplanen at dokumentasjon, rutiner, skjema og annen relevant beredskapsdokumentasjon finnes i kommunens kvalitetssystem EQS, mens oversikt over brukere og ressurser finnes i krisestøtteverktøyet RAYVN.

Tabell 2: Oversikt over vedlegg til overordnet beredskapsplan i Rana kommune

Navn på vedlegg	Beskrivelse
Vedlegg 1 - Varslingsliste kriseledelsen	Kontaktinformasjon for alle medlemmer av kriseledelsen og deres varaer. Sikrer rask mobilisering ved uønskede hendelser.
Vedlegg 2 - Kontaktpunkter og møteplasser	Rutiner for kontakt mellom kriseledelsen og befolkningen ved kriser, med 15 møteplasser og lokale kontaktpersoner ("kjentmenn").
Vedlegg 3 - Situasjonsrapportering	Mal for situasjonsrapporter med fem hovedelementer: situasjonsbilde, mediebilde, iverksatte tiltak, forventet utvikling og vurderte tiltak.
Vedlegg 4 - Evakueringsplan	Evakueringsplanen inneholder de ulike etaters ansvar, roller og oppgaver, samt oversikt over samarbeidsaktører, transportressurser og ulike bygg som kan benyttes ved evakuering. Plan for håndtering av evakuering i fire faser. Definerer ansvar for politi, kommune, nabokommuner og frivillige organisasjoner.
Vedlegg 5 - Plan for opplæring og øvelser	Definerer opplæringskrav og kompetansebehov. Øvelsesplan for 2024-2027 med 11 planlagte øvelser basert på scenarioene fra H-ROS.
Vedlegg 6 - Beredskapsråd	Etablerer et samarbeidsorgan mellom Rana kommune, statlige myndigheter, privat næringsliv og frivillige organisasjoner. Møtes minimum årlig.

Vedlegg 7 - Tiltakskort kriseledelsen	Operativ sjekkliste med konkrete handlinger for kriseledelsen ved hendelser. Inneholder tiltakskort for kommunedirektør og sektordirektører.
Vedlegg 8 – Plan for krisekommunikasjon	Todelt plan: operativ del for kommunikasjon i kriser, med umiddelbare tiltak, tiltakskort og kontaktlister. Videre, del om bakgrunn og beskrivelse av prinsipper for kommunikasjon med befolkning, media og egne ansatte.
Vedlegg 9 - Evaluering	Mal for evaluering av øvelser og hendelser med identifisering av læringspunkter og oppfølgingstiltak.
Vedlegg 10 - Loggføringsskjema	Manuelt skjema for loggføring når krisestøtteverktøyet RAYVN ikke er tilgjengelig.
Vedlegg 11 - Atomberedskapsplan	Beredskapsplan for håndtering av ulykker eller hendelser med fare for radioaktivt utslipp. Atomberedskapsplanen for Rana kommune 2024 er en integrert del av kommunens overordnede beredskapsplanverk og identifiserer tiltak som danner utgangspunkt for kommunens planlegging av atomberedskapen.
Vedlegg 12 - Mal liaisonavtale	Mal for avtale om liaison-personer som fungerer som bindeledd mellom kommunen og eksterne aktører under hendelser.
Vedlegg 13 – Helhetlig RanaROS	Kommunens helhetlige risiko- og sårbarhetsanalyse (RanaROS 2022–2025), vedtatt av kommunestyret 10. november 2022 (se 3.3.2). Danner grunnlaget for kommunens beredskapsplanverk og oppfølgingsplan.

Prosess for utarbeidelse, oppdatering og revisjon av beredskapsplanverket

Prosessen for utarbeidelse av beredskapsplaner i Rana kommune er forankret i den helhetlige risiko- og sårbarhetsanalysen. Det går fram at kommunen utarbeider en overordnet beredskapsplan og en oppfølgingsplan basert på helhetlig ROS, som spesifiserer konkrete tiltak, ansvarlige og tidsfrister for implementering.

I intervju kom det fram at den strategiske delen av den overordnede beredskapsplanen ligger fast, mens operative vedlegg oppdateres jevnlig, herunder blant annet varslingslister, oppmøteplasser, evakueringsplan og atomberedskap. Kommunen benytter kvalitetssystemet EQS til all internkontroll, herunder beredskap, og systemet gir automatisk varsling til dokumentansvarlig når det er tid for oppdatering. Dokumentansvarlig har ansvar for å gjennomgå endringsbehov og oppdatere dokumentet, og oppdateringer loggføres i EQS med ny dato og begrunnelse. Kommunen har videre utarbeidet en egen prosedyre for dette, samt et plan- og styringssystem som beskriver hvordan planverket er bygd opp, når det skal rulleres og på hvilket nivå. I intervju kom det ikke fram informasjon som tyder utfordringer knyttet til at ansatte mangler kjennskap til beredskapsplanverket.

Rana kommune har fastsatt at den overordnede beredskapsplanen skal revideres årlig, og at oppdatert versjon skal sendes Statsforvalteren og andre samarbeidsparter som politi, brann og helse. Sektorplanene skal revideres minimum hvert fjerde år og oppdateres ved endringer i risiko- og sårbarhetsbildet. Spesialiserte beredskapsplaner skal revideres etter behov. Kommunedirektøren ved beredskapskoordinator er ansvarlig for oppdatering av den overordnede beredskapsplanen, mens sektorene er ansvarlige for egne planer.

Oppfølging av tiltak relatert til beredskapsplanene følger samme prosess som tiltak knyttet til ROS. Evalueringen etter Øvelse Nordland 2023 viser at Oppvekst/kultur påpekte at beredskapsplanen var laget før skoler og barnehager ble heldigitale, og at det trengs oppdaterte retningslinjer for bortfall av strøm, telekom og EKOM. Revidering av sektorplan og avdelingsplaner for oppvekst og kultur ble registrert som oppfølgingstiltak, med planlagt ferdigstillelse i oktober 2024. Status per november 2025 er at arbeidet fortsatt pågår, og gjeldende sektorplan fremdeles er fra 2017 (jf. Tabell 1).

3.3.4 Kapasitet, kompetanse og øvelser

Kapasitet i beredskapsarbeidet

Kommunen har en sentral beredskapskoordinator som arbeider med beredskap på overordnet nivå, og som samarbeider med beredskapskoordinatorer i hver sektor. Ledelsens gjennomgang for 2024 peker på at økt risikobilde krever mer tid og ressurser, og har identifisert *«vurdering av organiseringen»* som et innsatsområde for 2025–2026. Det foreligger ingen formell analyse av kapasitet eller kompetansebehov per nivå eller rolle.

I intervju blir det pekt på at den sentrale beredskapskoordinatoren har en begrenset stillingsandel til beredskapsarbeid, og at sektorenes beredskapskoordinatorer ivaretar beredskapsoppgavene som en del av sine ordinære stillinger. Det er ikke dokumentert hvor store stillingsandeler som er satt av til rollene som beredskapskoordinatorer.

I intervju kommer det fram ulike vurderinger av kapasiteten til beredskapsarbeidet. Ved alvorlige hendelser vurderes kapasiteten som tilstrekkelig, ettersom ordinært arbeid legges til side og beredskapsarbeid prioriteres. Når det gjelder det forebyggende beredskapsarbeidet er det ulike meninger, og enkelte peker på at kapasiteten er utilstrekkelig gitt fagfeltets bredde og kompleksitet.

Opplæring, øvelser og kompetanseutvikling

Av vedlegg 5 til overordnet beredskapsplan fremgår det at ansvar for opplæring av ansatte følger linjeorganisasjonene, og at opplæringen skal omfatte roller og ansvar, varslingsrutiner og bruk av krisestøtteverktøy. Opplæringsplanen inneholder videre en tabell som viser hva slags kompetanse, øvelsestype, øvelsesmål og øvelsesfrekvens for hver av de de ulike rollene som er involvert i beredskapsarbeidet (KKL, krisestab, ledere, beredskapsrådgiver, loggfører, beredskapskoordinatorer i sektorene, beredskapsgrupper i sektorene, beredskapsrådet og folkevalgte). Opplæringsplanen inneholder også en øvingsplan som viser at det skal gjennomføres skrivebords-/funksjonsøvelser for hvert av de elleve scenarioene i ROS i løpet av perioden 2024-2027.

I forbindelse med verifisering opplyser kommunen at opplæring inngår som en del av det helhetlige og systematiske beredskapsarbeidet, og at øvingsplanen er et utgangspunkt som kan justeres etter reelt behov. Kommunen redegjør for opplæringen per rolle som følger:

- Kriseledelsen øves årlig i forbindelse med Øvelse Nordland (dokumentert i EQS), deltar på beredskapsdagen og har deltatt på opplæring i proaktiv kriseledelse med ekstern aktør (2021).

- Krisestaben deltar på årlige Øvelse Nordland og andre sektorøvelser (dokumentert i EQS), samt lederopplæringer via Teams.
- Sentral beredskapskoordinator deltar på det meste av øvelser både i egen regi og i regi av statsforvalter og andre eksterne aktører.
- Loggfører krisestab og beredskapskoordinatorer i sektorene deltar på månedlige møter i beredskapsnettverket og øvelser/kurs.
- Beredskapsgrupper i sektorene deltar på øvelser i egen sektor koordinert av beredskapskoordinator.
- Beredskapsrådet deltar på beredskapsdagen, ved utarbeidelse av H-ROS og overordnet planverk.
- For folkevalgte opplyser kommunen at opplæring ikke har vært gjennomført, men at de har fått H-ROS og overordnet planverk til behandling.

I intervju ble det pekt på at det gjennomføres jevnlig grunnopplæring for ledere i de nevnte temaene, men at det samtidig oppleves å være behov for sterkere systematisering og sektortilpasset opplæring som reflekterer ulike lovkrav og sektorspesifikke risikobilder og -scenarier.

Kommunen har etablert en rutine for gjennomføring av beredskapsøvelser som beskriver formål, ansvar, omfang og ulike øvelsestyper. Rutinen fastsetter at alle sektorer og avdelinger skal ha en øvingsplan forankret i lovverk og forskrifter, og at øvingsplanen skal inngå som en del av sektorenes beredskapsplanverk. Gjennomgangen viser at helse og mestring, samt teknisk, har etablert planer for øvelser, mens planer for øvrige sektorer er under utarbeidelse.

Gjennomgangen viser videre at kommunen har gjennomført flere øvelser, kurs og opplæringstiltak i perioden 2023–2025, og oversikt over gjennomføre øvelser i perioden 2023-2025 fremgår av Tabell 3.

Tabell 3: Gjennomførte øvelser og reelle hendelser i perioden 2023-2025[18]

Øvelse/hendelse	Tidspunkt	Kort beskrivelse
Januarkulde	16. januar 2026	Skrivebordsøvelse. Øvde samarbeidsavtalen med Meyergården hotell om opprettelse og drift av evakuerte- og pårørendesenter, og samhandling med politi, sykehus og frivillighet.
Reell hendelse – EKOM-bortfall	Desember 2025	To reelle hendelser med bortfall av elektronisk kommunikasjon 13.-14. desember og 27.-29. desember 2025. På det meste var 80% av basestasjonene ute av drift grunnet kraftutfall og fiberbrudd. Evaluert med 34 identifiserte forbedringstiltak.
Reell hendelse – Brann	12. desember 2025	Reell brannhendelse. Hendelsen ble håndtert i linjen uten at kommunal kriseledelse (KKL) ble satt. Evaluert med deltakelse fra politi, Røde Kors og andre involverte aktører.
Ekstremvær evakuering av pasienter	4. november 2025	Funksjonsøvelse med scenario evakuering av pasienter fra Helgelandssykehuset Mo i Rana til Selfors sykehjem. Øvde

[18] Listen viser de øvelsene som går fram av dokumentasjonen revisjonen har mottatt.

		samarbeidsavtalen om evakuering mellom Rana kommune og Helgelandssykehuset.
Varslingsøvelse – atomberedskap	Juni 2025	Varslingsøvelse knyttet til atomberedskapsplanverket.
Øvelse – kvikkleireskred	April 2025	Intern øvelse med scenario kvikkleireskred, gjennomført sammen med Helgelandssykehuset og interne aktører.
Mobilisering EPS og bruk av Ravyn	28. april 2025	Funksjonsøvelse. Trening på planverk for evakuerte- og pårørendesenter (EPS) med fokus på mobilisering og varsling, samt øving av nytt verktøy i RAYVN for registrering av pårørende og evakuerte.
Beredskapsdag 2025 – «Helhetlig beredskapsarbeid»	13. mars 2025	Årlig beredskapsdag med tema helhetlig beredskapsarbeid, arrangert i kommunestyresalen.
Øvelse Nordland 2025	29. januar 2025	Spilløvelse med scenario knyttet til større ulykke på Trænafestivalen. Nabokommunene Hemnes, Nesna, Lurøy og Træna deltok via Teams.
Brann ved Gruben sykehjem	11. desember 2024	Funksjonsøvelse med øving av krisestøtteverktøyet RAYVN og evakuering av institusjon.
PLIVO-øvelse (observatør)	2024	Kommunen deltok som observatører på PLIVO-øvelse.
Sikkerhetsdag NAV Rana	24. oktober 2024	Diskusjons- og spilløvelse med tema kjennskap til sikkerhetsrutiner, risikovurdering av brukermøter, håndtering av situasjoner med trusler og vold, samt ivaretakelse av ansatte etter hendelser.
Øvelse – atomberedskap	18. oktober 2024	Øvelse i atomberedskapsplanverket.
IKT-skrivebordsøvelse	12. oktober 2024	Skrivebordsøvelse med ekstern øvingsleder fra Sikri AS, med scenario inspirert av ransomware-angrepet mot Østre Toten kommune.
Øvelse Nordland 2024	5. april 2024	Spilløvelse med scenario ekstremvær/værhendelse. Involverte kommunens kriseledelse, nabokommunene Nesna, Træna og Lurøy, samt Heimevernet, Røde Kors, politiet og Sivilforsvaret.
Reell hendelse – «Ingunn»	Februar 2024	Reell værhendelse som ga kommunen anledning til å teste planverket under faktiske forhold.
Beredskapsdag 2024 – «Sikkerhet først»	22. februar 2024	Årlig beredskapsdag med tema sikkerhet, med bidrag fra Sivilforsvaret og nødetatene.
Kurs – radiac-målere	20. november 2023	Kurs for brann og redning på nyinnkjøpte radiac-målere.
Svikt i vannforsyning	08.november 2023	Funksjonsøvelse med gjennomgang og øving av beredskapsplan, kontroll av grad av egenberedskap, varsling og oppgaveløsning, samt krisehåndtering og samvirke internt i kommunen.
IUA-øvelse «Draugen»	21.–22. mars 2023	Kommunen deltok på IUA-øvelse «Draugen» i regi av interkommunalt utvalg mot akutt forurensning.
Øvelse – evakuering med Sivilforsvaret	23. mars 2023	Evakueringsøvelse gjennomført sammen med Sivilforsvaret. Det ble sendt ut befolkningsvarsling til boligområder på Gruben og Ytteren.

Beredskapsdag 2023 – «Årvåkenhet i en urolig tid»	15. februar 2023	Årlig beredskapsdag for beredskapsaktører i Rana med tema årvåkenhet i en urolig tid.
Øvelse Nordland 2023	27. januar 2023	Spilløvelse i regi av Statsforvalteren i Nordland, gjennomført sammen med nabokommunene Nesna, Lurøy, Rødøy og Træna, samt HV-14. Scenario med eskalering av cyberangrep mot kritisk infrastruktur i kontekst av hybride trusler, som medfører stans i nasjonalt transmisjonsnett (420kV), sporadisk utfall av mobilnett, og at Nets betalingsløsninger og BankID er nede.

I 2024 ble det gjennomført øvelser innen temaene ekstremver og langvarig strømbrudd, PLIVO (som observatør) og atomulykke i henhold til øvelsesplanen. I 2025 sto kvikkleireskred, flystyrt og pandemi på øvingsplanen, og av disse ble øvelse kvikkleirskred gjennomført, mens flystyrt og pandemi ikke ble gjennomført.

I intervju ble det pekt på at kommunen planlegger en fullskalaøvelse i forbindelse med nasjonal totalforsvarsøvelse i september 2026, med scenario for bortfall av e-kom og strøm/nett, befolkningsinformasjon, åpning og drift av møteplasser og operativ informasjonsinnhenting. Et sentralt mål er å gjøre møteplassordningen praktisk kjent og operativ, da den hittil primært har vært etablert på papiret.

Evaluering og forbedring

Den overordnede beredskapsplanen inneholder en mal for evaluering av øvelser og hendelser, som legger opp til en strukturert gjennomgang med identifisering av læringspunkter og oppfølgingstiltak med ansvarlig og frist. Evalueringer registreres i EQS, og systemet gir e-postpåminnelser nær frist. I den årlige ledelsens gjennomgang gjennomgås mål og forventninger, forbedringer og oppfølging av tiltak, og det kontrolleres at arbeidet følger lov og forskrift. Det fremkommer i intervju at det ikke er etablert en fast rutine for å omsette funn fra evalueringer til oppdatering av planverk. Det vises til at tilbakemeldinger fra de operative nivåene er viktige å få identifisert og innarbeidet i planverket, men det er noe personavhengig om og hvordan dette faktisk skjer.

Etter Øvelse Nordland 2024 ble det identifisert behov for revisjon av overordnet beredskapsplanverk, krisekommunikasjonsplan og flere sektorplaner, og det ble iverksatt en rekke konkrete oppfølgingstiltak. Evalueringen viste at samarbeid med nabokommuner via Teams fungerte godt, og at sektorene hadde god kontroll på sine tjenester og beredskapsplanverk.[19] Etter Øvelse Nordland 2025 ble det identifisert behov for å avklare ansvar for evakuering og loggføring, samt å sjekke funksjonalitet i varslingssystemet RAYVN. Dokumentasjonen fra begge øvelsene viser at kommunen har et etablert system for oppfølging av identifiserte tiltak, der hvert tiltak registreres i kvalitetssystemet med ansvarlig og frist, og gjennomføring godkjennes før saken lukkes.[20]

Evalueringsrapporten etter bortfall av elektronisk kommunikasjon (EKOM) i desember 2025 dokumenterer hendelsesforløpet, oppsummerer erfaringer fra de involverte, og identifiserer 34 forbedringstiltak med ansvarlig og frist. Tiltakene følges opp i kvalitetssystemet EQS. Statusoversikt fra kvalitetsportalen per april 2026 viser at 32 tiltak

[19] *Sektorplan beredskap for tekniske tjenester 2024-2027 Rana kommune*.
Vedtatt av kommunaldirektør tekniske tjenester 20.9.2024.

er registrert, hvorav om lag en tredjedel er under godkjenning og to tiltak er ferdigstilt. De resterende tiltakene, som utgjør i overkant av en tredjedel, er ikke påbegynt av ansvarlig selv om fristene er passert.

3.3.5 Samhandling og samarbeid

Intern samhandling

I den overordnede beredskapsplanen går det fram at Rana kommune har et internt beredskapsnettverk bestående av sentral og lokale beredskapskoordinatorer, kommunikasjonssjef, personvernombud og øvrige sektorrepresentanter. Nettverket, som ledes av beredskapskoordinator, møtes om lag månedlig og har ansvar for koordinering av planverk, kompetansebygging og planlegging av den årlige beredskapsdagen. Nettverket har ingen beslutningsmyndighet, men fungerer som en koordinerende arena for informasjonsflyt og praktisk samhandling på tvers av sektorene. Sektorenes beredskapskoordinatorer ivaretar tilsvarende funksjon innad i sine respektive sektorer.

Overordnet beredskapsplan beskriver forskjellen på kommunal kriseledelse (KKL) og krisestab på sektornivå, og hva som kjennetegner hendelser der KKL skal settes. Det er seks ulike kriterier, blant annet at hendelsen krever samhandling gjennom at den involverer flere sektorer/ansvarsområder eller støtte fra eksterne aktører.

I intervju kommer det fram at intern samhandling ved hendelser i stor grad skjer i linjeorganisasjonen, uten at KKL settes. Kommunen er en relativt stor organisasjon med ressurser til å håndtere mange hendelser på sektornivå, og KKL opplyses å bli satt sjeldnere enn i mange andre kommuner. Kommunaldirektørene har løpende dialog med kommunedirektøren ved hendelser, og behovet for å sette KKL vurderes fortløpende. Det oppleves som tydelig i organisasjonen på hvilket nivå hendelser skal håndteres, og at ting skal løses i tjenestene så langt det lar seg gjøre. Det pekes på at erfaringer fra reelle hendelser, herunder brannen 12. desember 2025 og EKOM-bortfallene 27.–29. desember 2025, viser at sektorene håndterte hendelsene i linjen uten at KKL ble satt. Ved EKOM-hendelsene ble det etablert krisestaber i de berørte sektorene, og dette ble vurdert som hensiktsmessig.

Evalueringsrapporten etter EKOM-bortfallene i desember 2025 viser flere eksempler på utfordringer knyttet til koordinering, informasjonsflyt og samhandling mellom sektorene og med eksterne aktører:

- Helgelandssykehuset konkluderte med at utfordringene var knyttet til kommunikasjon og samhandling mellom sykehuset, kommunen og innbyggere, og måtte lete etter alternative kontaktveier for å nå kommunen.
- Brann og redning fikk ikke beskjed om at nødnettet var nede, og oppdaget dette selv. Kommunikasjon ble improvisert via Messenger og WiFi.
- VA-avdelingen mistet all kommunikasjon med driftsovervåkingssystemet, og personellet fikk ikke tak i hverandre. De måtte oppsøke hverandre fysisk, og ville ikke hatt mulighet til å varsle abonnenter dersom det hadde oppstått alvorlige feil.
- Helse og mestring sjekket hvilke kommunikasjonskanaler som var tilgjengelige da de ordinære kanalene falt bort, og benyttet de som fungerte – herunder prioriterte SIM-kort

og fysisk oppmøte. Seksjonsleder kjørte fysisk til brann og redning for å sjekke status på nødnettet.
- Informasjon til befolkningen kom først i gang sent på kvelden, etter at legevakten tok kontakt med kommunikasjonssjefen via Messenger.

Ekstern samhandling

I vedlegg 6 til den overordnede beredskapsplanen er det fastsatt at Rana kommune skal ha et beredskapsråd. **Beredskapsrådet** er et samarbeidsorgan mellom kommunen, statlige myndigheter, privat næringsliv, frivillige lag og organisasjoner, og har som formål å ivareta samvirkeprinsippet. Rådet skal fungere som et forum for gjensidig informasjon og et rådgivende organ for kriseledelsen.

Beredskapsrådet ledes av ordfører og har en bred sammensetning med representanter fra kommunens ledelse og administrasjon samt eksterne aktører som politi, Heimevernet, Sivilforsvaret, Helgelandssykehuset, kraftselskap, teleselskap, industriaktører, frivillige organisasjoner og nabokommuner. Rådet skal innkalles minimum én gang årlig og har som formål å ivareta samvirkeprinsippet gjennom tverrfaglig informasjonsutveksling, felles situasjonsforståelse og koordinering av beredskapsplaner og øvelser.

Beredskapsrådet er formelt etablert gjennom politisk vedtak av 1. april 2014 og videreført i revidert planverk. I intervju ble det pekt på at beredskapsrådet har vært inaktivt over noe tid, men at aktørene har vært involvert i ROS-arbeid og øvelser. Ordfører har tatt initiativ til å reetablere rådet med møter én til to ganger i året. I forbindelse med verifisering opplyser Rana kommune at det arbeides med en avklaring på om spørsmålet om reetableringen og møtehyppighet skal behandles som politisk sak i kommunestyret eller om det kan opprettes direkte.

Rana kommune arrangerer en årlig **beredskapsdag**, som er en faglig møteplass og læringsarena for kommunens beredskapsaktører. Dagen har vært gjennomført årlig i snart 10 år, planlegges av beredskapsnettverket og streames slik at alle ansatte kan følge med. Beredskapsdagen sikrer at relevante aktører møtes fast minst én gang i året, og fungerer som en arena for kompetanseheving og nettverksbygging uavhengig av andre formaliserte samarbeidsstrukturer.

Rana kommune har inngått en rekke **samarbeidsavtaler** med eksterne aktører som kan benyttes i håndteringen av ulike hendelser.[21] Avtalene omfatter blant annet samarbeid med frivillige organisasjoner om bistand ved evakuert- og pårørendesenter, avtale med Helgelandssykehuset om gjensidig evakuering av pasienter, og beredskapshotellavtale.

Beredskap for helse- og mestring 2023 – 2027. Plan. Vedtatt av kommunestyret 20.05.2014, revidert og administrativt vedtatt 25.01.2023., Rana kommune. *Beredskapsplan Støttetjenesten 2025-2027*. Vedtatt og sist revidert av kommunaldirektør stab 15.10.2025. *Sektorplan for beredskap i skoler og barnehager 2017-2018*. Vedtatt av utvalg for oppvekst og kultur 25.01.2017.
og Helgelandssykehuset. *Avtale om evakuering mellom elgelandssykehuset og Rana kommune*. Signert 11.06.2025., NRK, Telenor, Norkring og Norsk Lokalradioforbund. *Samarbeidsavtale om lokal- og riksradiostasjoners virksomhet under kriser og katastrofer*. Signert 2018., Rana kommune, Scandic Meyergården. *Samarbeidsavtale Scandic Meyergården Hotell og Rana kommune – Beredskapshotell*. Signert 07.08.2025.

Alle avtalene inneholder bestemmelser om varsling, roller og ansvar, økonomi og forsikring, og revideres jevnlig.

I tillegg deltar kommunen i **interkommunalt samarbeid** gjennom Polarsirkelrådet,[22] der det er etablert en felles regional beredskapskoordinator for Nord-Helgeland for perioden 2025–2027. Koordinatoren, som startet i oktober 2025, skal samordne kommunene til likt nivå, harmonisere planverk og tilrettelegge for felles øvelser. I intervju ble ordningen omtalt som nyttig, særlig for de mindre kommunene i regionen som ikke har tilstrekkelig kapasitet eller kompetanse til å håndtere hendelser på egenhånd. Det ble videre vist til at ordføreren har tatt initiativ til å etablere et interkommunalt beredskapsråd i Polarsirkelrådet.

I intervju beskrives samarbeidet med blålysetater, Røde Kors, Heimevernet og andre frivillige organisasjoner som godt fungerende ved både øvelser og faktiske hendelser. Kommunedirektøren vurderer samhandlingen med blålysetatene som meget god, og peker på at det har vært en forbedring over tid som skyldes felles øvelser, evalueringer og oppfølging av konkrete tiltak. Evalueringen etter brannen i romjulen 2025 ble gjennomført med deltakelse fra politi, Røde Kors og andre involverte aktører, og det er etablert god rolleforståelse og kontakt mellom de ulike etatene. Kommunen gjennomfører tverretatlige øvelser, herunder PLIVO-øvelser med nødetatene, og brann og redning har en fast øvelsesplan med planlagte samøvelser med eksterne aktører. Brannsjefen peker på at det er en suksessfaktor for større øvelser at eksterne aktører involveres tidlig i planleggingsprosessen for å definere felles mål.

3.4 Vurderinger

3.4.1 Roller og ansvar i beredskapsorganiseringen

Deloitte vurderer at Rana kommune har definert roller og ansvar i beredskapsorganiseringen i tråd med forskrift om kommunal beredskapsplikt § 4. Det er tydelig at sektorene har ansvar for beredskapen innenfor sitt ansvarsområde, og den overordnede beredskapsplanen definerer hvilke typer situasjoner som skal medføre eskalering til kommunal kriseledelse (KKL). Både KKL og beredskapsstabene sine roller og ansvar fremstår godt dokumentert og i samsvar med de beredskapsrettslige prinsippene om ansvar, nærhet, likhet og samvirke. Kommunen har videre etablert tydelige rutiner for rapportering av hendelser, herunder flytskjema som understøtter ansattes rapportering oppover i organisasjonen.

Undersøkelsen viser at det er noe uklart når og hvordan sentral beredskapskoordinator skal involveres i håndteringen av hendelser som oppstår i sektorene. Deloitte mener at dette bør tydeliggjøres i planverket, for å sikre at koordinators kompetanse og helhetsperspektiv bringes inn i sektorarbeidet ved behov. Dette vil kunne bidra til at kommunen utnytter kompetanse og tilgjengelige ressurser på en bedre måte, og redusere risikoen for at for at hendelser som krever samhandling på tvers håndteres på for lavt nivå uten tilstrekkelig informasjonsflyt. Deloitte merker seg også at hverken sentral eller sektorenes beredskapskoordinatorer sine roller og ansvar er omtalt i overordnet beredskapsplan, og mener dette bør omtales i overordnet planverk ettersom personene

[22] Rana kommune og Røde Kors Rana. *Samarbeidsavtale om beredskap mellom Rana kommune og Rana Røde Kors*. Avtale. Signert 20.10.2021.

har en sentral rolle i beredskapsorganisasjonen, jf. forskrift om kommunal beredskapsplikt § 4a.

3.4.2 Risiko- og sårbarhetsanalyser

Deloitte vurderer at Rana kommune har gjennomført og dokumentert en helhetlig risiko- og sårbarhetsanalyse i tråd med kravene i sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt § 2. Analysen er forankret i kommunestyret, utarbeidet etter DSBs veileder og identifiserer 11 uønskede hendelser med vurderinger av sannsynlighet, sårbarhet og konsekvenser. Det er etablert rutiner for oppdatering med fullstendig revisjon hvert fjerde år, og neste revisjon er planlagt i 2026 i samsvar med forskrift om kommunal beredskapsplikt § 6.

Kommunen har etablert et system for oppfølging av risikoreduserende tiltak gjennom kvalitetssystemet EQS og den årlige ledelsens gjennomgang. Undersøkelsen viser likevel at ikke alle tiltak er fulgt opp, noe som opplyses å skyldes begrenset kapasitet, manglende oversikt grunnet systembytte og helhetlig økonomisk prioritering. Deloitte anbefaler at kommunen vurderer om rutinene for oppfølging av tiltak er tilstrekkelige for å sikre at tiltak blir utført innen de fastsatte fristene (jf. kommuneloven § 25-1).

3.4.3 Beredskapsplanverk

Deloitte vurderer at Rana kommune har etablert et overordnet beredskapsplanverk som i hovedsak oppfyller kravene i sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt § 4. Planverket er strukturert i tre nivåer og inneholder samtlige av de påkrevde elementene, herunder plan for kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for krisekommunikasjon.

Når det gjelder beredskapsplanverkets dekning av risikoområdene, viser undersøkelsen at sektorene skal håndtere hendelser innenfor sine respektive ansvarsområder, og at KKL skal settes dersom hendelsen krever samhandling på tvers av sektorer eller støtte fra eksterne aktører. Etter Deloittes vurdering er dette i samsvar med ansvarsprinsippet og likhetsprinsippet. Videre vurderer Deloitte at utformingen av overordnet beredskapsplan er i samsvar med DSBs veileder til forskrift om kommunal beredskapsplikt, som anbefaler en generisk tilnærming («*all hazard approach*»), slik at beredskapsplanen kan legges til grunn uavhengig av hvilken hendelse som måtte inntreffe.

Samtidig vurderer Deloitte at kommunen har et forbedringspotensial når det gjelder samordningen mellom de ulike beredskapsplanene. DSB anbefaler i sin veileder at overordnet beredskapsplan samordner og integrerer andre beredskapsplaner, og gir en struktur som viser sammenhengen mellom det overordnede planverket og beredskapsplaner innenfor ulike fagområder. Rana kommunes overordnede beredskapsplan omtaler ikke de øvrige planene i kommunen eller forholdet mellom dem. Etter Deloittes vurdering svekker dette planens funksjon som samordnende dokument, jf. forskrift om kommunal beredskapsplikt § 4.

Det er positivt at kommunen har utarbeidet en prosedyre for revisjon av planverket og benytter EQS med automatisk varsling til dokumentansvarlig. Undersøkelsen viser likevel at planverket ikke er revidert i samsvar med egne frister, og at sektorplan for oppvekst og kultur fortsatt ikke er ferdigstilt, selv om ferdigstillelse ble registrert som oppfølgingstiltak

med frist oktober 2024. Etter Deloittes vurdering er det en svakhet at en hel sektor mangler et eget beredskapsplanverk.[23]

Undersøkelsen viser videre at beredskapsplanene er lagret i ulike mapper i EQS, at planer og rutiner er lagret om hverandre, og at enkelte enheter har kontinuitetsplaner som ikke ligger i kvalitetssystemet. Etter Deloittes vurdering svekker dette kommunens samlede oversikt over beredskapsplanverket og vanskeliggjør kontroll med at planene holdes oppdaterte, jf. forskrift om kommunal beredskapsplikt § 9. Deloitte merker seg for øvrig at det ikke fremkommer data som tyder på at ansatte mangler kjennskap til det beredskapsplanverket som gjelder dem.

3.4.4 Kapasitet, kompetanse og øvelser

Undersøkelsen viser at Rana kommune har etablert en beredskapsorganisasjon bestående av KKL, krisestaber i sektorene, beredskapskoordinatorer og en linjeorganisasjon som ivaretar hendelser på sektornivå. Kapasiteten til å håndtere alvorlige hendelser opplyses å være tilstrekkelig, og kommunen har vist evne til å håndtere reelle hendelser i linjeorganisasjonen. Undersøkelsen viser samtidig at kapasiteten til det forebyggende beredskapsarbeidet vurderes ulikt internt. Deloitte anbefaler at kommunen vurderer om kapasiteten til forebyggende beredskapsarbeid er tilstrekkelig for å sikre et systematisk samfunnssikkerhetsarbeid over tid, jf. forskrift om kommunal beredskapsplikt § 1 og DSBs veileder som understreker at systematisk arbeid og gode interne kvalitetssikringsrutiner sikrer at beredskapsarbeidet er oppdatert og utvikles i tråd med kommunens utfordringer.

Kommunen har gjennom vedlegg til overordnet beredskapsplan etablert et rammeverk for opplæring med kompetansekrav og øvelsesfrekvens for de ulike rollene i beredskapsorganisasjonen, og det gjennomføres jevnlig grunnopplæring for ledere. Deloitte har samtidig identifisert forbedringspotensial knyttet til dokumentasjon av gjennomført opplæring. Opplæringen er ikke dokumentert på en måte som gjør det mulig å ettergå om alle med roller i krisehåndteringen har fått opplæringen planen forutsetter, jf. forskrift om kommunal beredskapsplikt § 7.

Rana kommune har gjennomført flere øvelser i perioden 2023–2025 med relevante scenarioer og deltakelse fra eksterne aktører, i tråd med forskrift om kommunal beredskapsplikt § 7. Undersøkelsen viser samtidig at øvingsplanen på overordnet nivå ikke er fulgt, ved at to av de tre planlagte øvelser for 2025 ikke ble gjennomført i tråd med planen. Videre har ikke alle sektorer ferdigstilt egne øvingsplaner i samsvar med kommunens retningslinjer. Deloitte anbefaler at kommunen sikrer at øvingsplanen blir fulgt og ved behov revidert, og at de sektorspesifikke øvingsplanene ferdigstilles og brukes aktivt, jf. kommuneloven § 25-1.

Kommunen har etablert rutiner for evaluering av øvelser og hendelser i samsvar med forskrift om kommunal beredskapsplikt § 8, og den årlige ledelsens gjennomgang gir en strukturert mekanisme for oppfølging av tiltak. Samtidig viser statusoversikten fra

[23] For skoler og barnehager gjelder i tillegg et selvstendig krav på virksomhetsnivå etter forskrift om helse og miljø i barnehager, skoler og skolefritidsordninger (F28.03.2023 nr. 449) § 14, som pålegger virksomheten planer og rutiner for å forebygge og håndtere skader, ulykker og andre alvorlige hendelser. Som eier av kommunale skoler og barnehager er kommunen direkte ansvarlig for at disse kravene oppfylles, jf. § 3.

kvalitetsportalen per april 2026 at i overkant av en tredjedel av tiltakene etter EKOM-hendelsene ikke er påbegynt, selv om fristene er passert. Deloitte vil understreke betydningen av at identifiserte læringspunkter følges opp systematisk, og at beredskapsplanverket oppdateres i tråd med funn fra evalueringer, jf. forskrift om kommunal beredskapsplikt § 8.

3.4.5 Samarbeid og samhandling

Etter Deloittes vurdering har Rana kommune etablert flere gode arenaer og strukturer for samarbeid og samhandling, herunder beredskapsnettverket og den årlige beredskapsdagen, i tråd med forskrift om kommunal beredskapsplikt § 1. Informasjon fra både evalueringer og intervju taler for at intern samhandling ved flere faktiske hendelser har fungert godt.

Samtidig avdekket EKOM-hendelsene i desember 2025 flere svakheter, herunder manglende varsling mellom sektorer og forsinket informasjon til befolkningen, noe som viser at samhandlingen er sårbar når ordinære kommunikasjonskanaler faller bort. Kommunal kriseledelse ble ikke satt under EKOM-hendelsene; det ble i stedet etablert krisestaber i de berørte sektorene. Overordnet beredskapsplan angir seks kriterier for når KKL bør settes, der det er tilstrekkelig at ett kriterium er oppfylt. Etter Deloittes vurdering fremstår flere av disse som oppfylt ved EKOM-hendelsene, noe som tilsier at spørsmålet om å sette KKL burde vært vurdert. Deloitte merker seg videre at evalueringsrapporten etter hendelsene ikke drøfter spørsmålet om KKL burde vært satt.

Kommunen har videre inngått samarbeidsavtaler med flere eksterne aktører, gjennomfører tverretatlige øvelser og deltar i interkommunalt samarbeid gjennom Polarsirkelrådet. Samarbeidet med blålysetater og frivillige organisasjoner beskrives som godt fungerende ved faktiske hendelser, og er forbedret over tid gjennom felles øvelser og evalueringer. Deloitte vurderer at kommunen har etablert et godt eksternt samarbeid i tråd med forskrift om kommunal beredskapsplikt § 5.

Deloitte merker seg at beredskapsrådet, som er formelt etablert gjennom politisk vedtak av 1. april 2014, har vært inaktivt i en lengre periode, noe som ikke samsvarer med anbefalingen i veileder til forskrift om kommunal beredskapsplikt § 5. Det er positivt at ordfører har tatt initiativ til å reetablere rådet, og at aktørene har vært involvert i ROS-arbeid og øvelser i mellomtiden. Deloitte anbefaler at kommunen følger opp reetableringen av beredskapsrådet som arena for formalisert samordning med eksterne aktører.

4 Håndtering av cyberangrep

4.1 Problemstillinger

I dette kapittelet vil vi svare på følgende hovedproblemstilling og underproblemstillinger:

2. **Har Rana kommune etablert tilstrekkelig beredskap for håndtering av uønskede digitale hendelser, under dette et cyberangrep mot et utvalgt kritisk system?**
   a) Er roller og ansvar tydelig definert og kommunisert?
   b) Har kommunen gjennomført og dokumentert risiko- og sårbarhetsanalyser som spesifikt omfatter IT-trusler mot et utvalgt kritisk system (som for eksempel malware, datainnbrudd, tjenestenektangrep (DDoS), og lekkasje av personopplysninger)?
   c) Er det utarbeidet beredskapsplaner og tiltakskort som er kjent blant relevante ansatte, og som inneholder konkrete prosedyrer for håndtering av IT-hendelser?
   d) Hvordan sikrer kommunen tilstrekkelig samhandling med eksterne aktører, som IT-leverandører og nasjonale sikkerhetsmyndigheter, under håndteringen av et cyberangrep mot et utvalgt kritisk system (jf. samvirkeprinsippet)?
   e) Er det iverksatt hensiktsmessige internkontrolltiltak for å redusere risikoen for uønskede digitale hendelser? Under dette tiltak knyttet til:
      i) Innlogging og sikkerhet
      ii) Tilgangsstyring
      iii) Oppdatering og vedlikehold
      iv) Sikkerhetskopi og gjenoppretting
      v) Opplæring av ansatte
      vi) Overvåking og varsling
   f) Har kommunen rutiner for å evaluere og forbedre sine digitale beredskapstiltak, basert på erfaringer fra faktiske hendelser eller øvelser relatert til IT-sikkerhet? Under dette; hvordan sikrer kommunen at den er tilstrekkelig oppdatert på nye digitale trusler som dukker opp?

4.2 Revisjonskriterier

Basert på krav i kommuneloven, forskrift om kommunal beredskapsplikt og NSMs grunnprinsipper for IKT-sikkerhet, har Deloitte utledet følgende revisjonskriterier knyttet til problemstillingen som undersøkes i dette kapitlet:

Tema	Revisjonskriterier (kommunen skal)	Kilde
Roller og ansvar	Utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering knyttet til digital sikkerhet og cyberberedskap, og kartlegge roller og ansvar for IKT-sikkerhet internt i	Kommuneloven § 25-1; NSM grunnprinsipp 1.3

	virksomheten og hos eksterne leverandører og partnere, herunder klargjøre hvem som skal kontaktes ved hendelser.	
Risiko- og sårbarhetsanalyser; beredskapsplanverk	Inkludere vurderinger av digitale trusler og IKT-sikkerhetsrisiko i den helhetlige risiko- og sårbarhetsanalysen, og gjennomføre risikovurderinger av nettverks- og informasjonssystemer som benyttes for å levere tjenester. ROS-vurderingene bør beskrive: • systemenes betydning for tjenesteleveransen, • hvilke hendelser systemene kan bli utsatt for, • hvilke sårbarheter som er knyttet til systemene, konsekvensen av hendelser, • og i hvilken grad kommunen er avhengig av andre virksomheter. ROS-analysen skal oppdateres med hensyn til digitale trusler og IKT-sikkerhet i takt med endringer i risikobildet, og ved endringer i kommunen som kan påvirke sikkerheten. ROS-analysen skal legge grunnlag for langsiktige mål, strategier, prioriteringer og plan for oppfølging av arbeidet med samfunnssikkerhet og beredskap, inkludert håndtering av uønskede digitale hendelser.	Sivilbeskyttelsesloven § 14; forskrift om kommunal beredskapsplikt §§ 2, 3 og 6; NSM grunnprinsipp 1.1 og 3.1
Roller og ansvar; Beredskapsplanverk; Samhandling; Krisekommunikasjon	Utarbeide en overordnet beredskapsplan som integrerer planer for håndtering av digitale hendelser og cyberangrep, med tydelig ansvar, roller og fullmakter, herunder rolle- og ansvarsbeskrivelse for personell som skal håndtere hendelser, ledere med beslutningsansvar på ulike nivåer, og beredskapsvakter som er tilgjengelige utenom normal arbeidstid og i ferieperioder. Planen skal inneholde: • varslingsliste over aktører med roller i krisehåndtering av cyberhendelser, inkludert digitale sikkerhetsansvarlige og relevante IKT-ressurser, der alle på listen er informert om sin rolle og har tilstrekkelig kompetanse, • ressursoversikt over IKT-ressurser og bistandsavtaler, • plan for krisekommunikasjon med befolkningen, media og egne ansatte, • samt varsling til Datatilsynet om hendelser som virker vesentlig inn på tjenesteleveransen.	Forskrift om kommunal beredskapsplikt § 4; NSM grunnprinsipp 4.1
Beredskapsplanverk; internkontrolltiltak	Iverksette teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, funksjon og risiko ved nettverk og informasjonssystemer, herunder tiltak for sterk	NSM grunnprinsipp 2.2, 2.4, 2.6, 2.9 og 3.2

	autentisering, tilgangsstyring, nettverkssegmentering, tiltak for gjenoppretting og sikkerhetsovervåking.	
Beredskapsplanverk; internkontrolltiltak	Utarbeide tiltakskort for håndtering av digitale hendelser, med prosedyrer for å opprettholde drift ved bortfall av digitale løsninger, inkludert reserveløsninger.	Sivilbeskyttelsesloven § 15; NSM grunnprinsipp 4.1 og 4.3
Samhandling	Arbeide systematisk og helhetlig med samfunnssikkerhetsarbeid på tvers av sektorer i kommunen, og etablere samarbeid med andre kommuner om lokale og regionale løsninger av forebyggende og beredskapsmessige oppgaver, med sikte på best mulig utnyttelse av de samlede ressursene. Kommunen bør øve i samarbeid med andre kommuner og relevante aktører der det er hensiktsmessig for å styrke håndtering av digitale kriser.	Forskrift om kommunal beredskapsplikt §§ 1, 5 og 7
Internkontrolltiltak	Ha et system for opplæring som sikrer at alle med roller i håndtering av digitale hendelser og IKT-beredskap har nødvendige kvalifikasjoner og kompetanse, og sikre at ansatte, leverandører og oppdragstakere er gjort kjent med relevante sikkerhetstiltak og får nødvendig opplæring ved behov. Kommunen skal sikre at det er tilstrekkelig kapasitet og kompetanse til arbeid med digital sikkerhet og cyberberedskap, blant annet gjennom å kartlegge behov for kompetanse via analyser og planer.	Forskrift om kommunal beredskapsplikt §§ 1, 4 c og 7; NSM grunnprinsipp 1.3 og 4.1
Evaluering og forbedring; Risiko- og sårbarhetsanalyse; Beredskapsplanverk	Etter gjennomførte øvelser og faktiske uønskede digitale hendelser evaluere krisehåndteringen, identifisere avvik og risiko for avvik, identifisere karakteren og omfanget av hendelsen, og sette i verk nødvendige mottiltak og tiltak for å gjenopprette den sikre tilstanden. Helhetlig ROS og beredskapsplaner skal oppdateres dersom evalueringer gir grunnlag for det. Kommunen skal gjennomføre beredskapsøvelser med scenario som omfatter cyberangrep og digitale trusler, basert på den helhetlige risiko- og sårbarhetsanalysen, for å teste planverket og utvikle kompetansen til å håndtere hendelser.	Forskrift om kommunal beredskapsplikt §§ 7 og 8; kommuneloven § 25-1; NSM grunnprinsipp 3.4, 4.1, 4.3 og 4.4

Se vedlegg 3 for utfyllende revisjonskriterier.

4.3 Datagrunnlag

4.3.1 Roller og ansvar

Kommunestyret har vedtatt en overordnet retningslinje for informasjonssikkerhet (K.sak 3/2024) som er det overordnede styringsdokumentet for informasjonssikkerhetsarbeidet i kommunen. Retningslinjen fastslår at kommunen skal ha en helhetlig tilnærming til

informasjonssikkerhet, at arbeidet skal være forankret i ledelsen, og at kommunen skal ha et styringssystem basert på ISO 27001. Kommunen har videre utarbeidet dokumentet «IKT-sikkerhet 2025-2026», som beskriver metode og tiltak for å sikre digital sikkerhet, og fastslår at ansvaret for informasjonssikkerhet følger linjeledelsen. Det er etablert en sikkerhetsorganisasjon med ansvar- og rollefordeling innenfor personvern- og informasjonssikkerhetsarbeidet, hvis sammensetning vurderes løpende og minst én gang per år i forbindelse med ledelsens gjennomgang.

IKT-avdelingens beredskapsplan definerer roller og ansvar i beredskapsstaben ved krisesituasjoner, herunder kriseledelse IKT (IKT-sjef), vara til kriseleder IKT (fagleder IKT-drift), rådgiver IKT-sikkerhet, nettverksansvarlig, ansvarlig for datarom, feltansvarlig, systemoversikt og henvendelseskoordinator. Alle ansatte på IKT-avdelingen vurderes også innkalt når beredskapsstab settes.

Når det gjelder kommunikasjonslinjer, fremgår det at IKT-sjef ved situasjoner/hendelser har ansvar for å orientere kommunaldirektør stab/støtte, og at de to i fellesskap skal vurdere om kommunedirektør må orienteres. Kommunedirektør beslutter om kriseledelsen skal settes, og beredskapsstab på IKT aktiveres etter anbefaling fra IKT-sjef. IKT-sjef leder beredskapsarbeidet på IKT og rapporterer og loggfører fortløpende i RAYVN.

Rana kommune har etablert en formalisert sikkerhetsorganisasjon for å ivareta arbeidet med informasjonssikkerhet og personvern. Ansvaret for informasjonssikkerhet innebærer både et overordnet ansvar for at kommunen har tilfredsstillende informasjonssikkerhet i henhold til gjeldende lovverk, og et ansvar for at ledere på alle nivåer, ansatte, innleid personell og leverandører etterlever de krav og plikter som gjelder i kommunen.

Sikkerhetsorganisasjonen består av følgende roller og nivåer: kommunedirektør (behandlingsansvarlig), kommunedirektørens ledergruppe, sikkerhetsansvarlig, sikkerhetsgruppen, systemeier (kommunaldirektør), avdelingsledere, systemansvarlig, ansatte, beredskapsleder og personvernombud. Rollene er nærmere beskrevet i tabellen nedenfor.

Tabell 4: Roller og ansvar knyttet til IT-sikkerhet og -beredskap

Rolle	Beskrivelse av rolle og ansvar
Kommunedirektøren og kommunedirektørens ledergruppe	Kommunedirektøren er behandlingsansvarlig og har det overordnede ansvaret for at informasjonssikkerheten i kommunen ligger på et forsvarlig nivå. Kommunedirektøren skal fastsette mål og strategi for informasjonssikkerhet, sørge for at kommunen har en sikkerhetsorganisasjon med ansvar for å etablere og iverksette et styringssystem for informasjonssikkerhet, og sikre tilstrekkelige ressurser – både personell og økonomi – slik at tilfredsstillende informasjonssikkerhet og personvern opprettholdes. Det daglige operative behandlingsansvaret for informasjonssikkerhet er delegert til systemeier (kommunaldirektør).
IKT-sjef	IKT-sjefens rolle i sikkerhetsgruppen innebærer å sørge for tilfredsstillende informasjonssikkerhet og personvern, herunder å bidra i prosessen med å gjennomføre risikovurderinger og opplæringstiltak, sikre at den daglige driften av kommunens datanettverk og IKT-systemer drives i samsvar med

	sikkerhetspolitikken, sørge for at det jevnlig foretas dokumenterte stikkprøver av driftslogger, og vedlikeholde IT-beredskapsplanen
Sikkerhetsansvarlig (rådgiver for personvern og informasjonssikkerhet)	Sikkerhetsansvarlig har ansvar for å sørge for en hensiktsmessig og velfungerende sikkerhetsorganisasjon, lede sikkerhetsgruppen, etablere og vedlikeholde kommunens internkontrollsystem for informasjonssikkerhet og personvern, gjennomføre sikkerhetsrevisjon, påse at det gjennomføres risikovurderinger og opplæringstiltak, og påse at avviksmeldinger følges opp
Sikkerhetsgruppen	Sikkerhetsgruppen er et rådgivende organ innen informasjonssikkerhet, behandling av personopplysninger og personvern, og ledes av sikkerhetsansvarlig. Sikkerhetsgruppen møtes månedlig, og består av: - Sikkerhetsansvarlig (rådgiver for personvern og informasjonssikkerhet) - Dokumentsikkerhet (arkivleder) - IKT-sikkerhet (IKT-sjef) - Fysisk sikkerhet (representant fra KF bygg) - Internkontroll (kvalitetsansvarlig) - Juridisk rådgiver - Representanter fra sektorene helse og omsorg, oppvekst og kultur og teknisk
CIKTSO-gruppen	I tillegg til sikkerhetsgruppen er det opprettet en gruppe kalt «CIKTSO»-gruppen, etablert som en forsterkning etter ledelsens gjennomgang 2024, i samråd mellom sikkerhetsansvarlig og IKT-sjef. Gruppen består av rådgiver for personvern og informasjonssikkerhet, IKT-sjef, en dedikert sikkerhetsrådgiver på IKT-avdelingen og to andre faste fra IKT-avdelingen. Foreløpig mandat til gruppen er basert på ansvarsområdet til en CISO, og målet er å sikre god og jevnlig dialog og fokus på IKT-sikkerhet for organisasjonen som helhet. CIKTSO-gruppen har møter hver 14. dag
Systemeier (kommunaldirektørene – én per sektor)	Systemeier (kommunaldirektør) har det daglige operative behandlingsansvaret for informasjonssikkerheten i den enkelte sektor delegert fra behandlingsansvarlig. Systemeier skal påse at gjeldende lovverk, instrukser og rutiner følges, gjennomføre årlig egenkontroll av informasjonssikkerheten i avdelingen, påse at avvik blir rapportert og fulgt opp, oppnevne og autorisere systemansvarlige, og sikre at forholdet til leverandører og andre eksterne aktører er i samsvar med gjeldende krav
Beredskapsleder (sentral beredskapskoordinator)	Beredskapsleder har ansvar for å påse at det er etablert tilfredsstillende planverk og beredskapstiltak innen informasjonssikkerhet og personvern, delta i ledelsens årlige gjennomgang, og delta i sikkerhetsgruppen ved behov

I intervju fremkommer det at IKT-avdelingen er i en omstillingsfase der systemer flyttes til en driftsleverandør og flere løsninger leveres som SaaS-tjenester[24]. Omstillingen har frigjort ressurser som er omdisponert til IKT-sikkerhet, og kommunen har nå en dedikert rådgiver for IKT-sikkerhet. IKT-sjefen understreker at kommunens samlede sikkerhetskompetanse må vurderes i et helhetsperspektiv som inkluderer både interne ressurser og tilknyttede eksterne aktører.

IKT-avdelingen har etablert en døgnkontinuerlig vaktordning som mottar henvendelser om potensielle sikkerhetshendelser og sikrer et umiddelbart kontaktpunkt ved hendelser. IKT-sjefen inngår ikke i kommunens krisestab, men IKT-avdelingen har en egen beredskapsplan som er avstemt med kommunens overordnede beredskapsplan.

[24] SaaS: Software as a Service.

I intervju fremkommer det at sikkerhetsarbeidet er organisert gjennom sikkerhetsgruppen, der sikkerhetstemaer tas opp jevnlig og alle sektorer er representert. CIKTSO-gruppen møtes hver 14. dag og arbeider med sikkerhetstiltak basert på informasjon fra eksterne kilder og egne funn.

Ledelsens gjennomgang for 2024 peker på at sikkerhetsorganisasjonen har mange sårbare roller og begrenset robusthet. Nøkkelpersoner besitter mye kompetanse, men er få sammenlignet med organisasjonens størrelse, og har ikke øremerket tid til sikkerhetsarbeidet. Det etterlyses større robusthet og flere dedikerte ressurser.

I intervju blir det pekt på at kommunen er bevisst på at nye risikoer, særlig innenfor IKT-sikkerhet, krever kompetanse kommunen ikke kan eller klarer å ha selv. Kommunen følger nasjonale sikkerhetsmyndigheters standarder, deltar i relevante fora og har etablert samarbeidsavtaler med leverandører og aktører som har nødvendig kompetanse, for å sikre tilgang på denne.

I intervju fremkommer det at ansvarsfordelingen mellom IKT-avdelingen, fagmiljøene i sektorene og ekstern driftsleverandør ikke er tilstrekkelig avklart på alle områder, og at risikovurderinger har vært gjennomført separat uten tilstrekkelig samhandling og koordinering. I forbindelse med verifisering bemerkes det at Rana kommune i 2025 gikk over fra lokal servertjeneste til eksternt tjenestekjøp, noe som har medført en overgangsfase med endring av rutiner og samhandling etter hvert som de ulike fagsystemene har blitt flyttet over. Dette er nærmere beskrevet i casegjennomgangen av Profil omsorg, jf. kapittel 4.3.7.

4.3.2 Risiko- og sårbarhetsanalyser

Rana kommune gjennomfører risikovurderinger på tre nivåer: helhetlig ROS (RanaROS 2022–2025) på overordnet nivå, en overordnet risikovurdering for IKT-sikring strukturert etter NSMs grunnprinsipper, og risikovurdering av det enkelte system ved anskaffelse og endringer, herunder personvernkonsekvensvurdering (DPIA) [25].

ROS-analysen for IKT-sikkerhet er strukturert etter NSMs grunnprinsipper og dekker kategoriene identifisere og kartlegge, beskytte og opprettholde, oppdage, og håndtere og gjenopprette[26]. For hvert risikomoment angis eksisterende risikoreduserende tiltak, sannsynlighet, konsekvens og risikonivå. Analysen viser at de fleste risikoene er vurdert til lav eller svært lav sannsynlighet, men at konsekvensene ved flere av momentene er vurdert som høye eller svært høye.

Ledelsens gjennomgang 2024 dokumenterer at kommunen har fokus på systematisk gjennomføring av risikovurderinger, men peker på et vedvarende etterslep av ROS- og DPIA-vurderinger, særlig ved anskaffelse av nye IKT-systemer og ved nye eller endrede behandlinger av personopplysninger. Det fremgår videre at arbeidet med en overordnet

[25] DIPA (Digital Protection Impact Assessment) er en vurdering av personvernkonsekvenser som skal gjennomføres når en behandling av personopplysninger kan medføre høy risiko for fysiske personers rettigheter og friheter, jf. personvernforordningen (GDPR) artikkel 35. Vurderingen skal blant annet beskrive den planlagte behandlingen, vurdere om behandlingen er nødvendig og forholdsmessig, og kartlegge risikoen for de registrertes rettigheter samt tiltak for å håndtere denne risikoen.

[26] vedlegg IKT-201-V2, datert 12. september 2025

ROS for informasjonssikkerhet og personvern er igangsatt, med deltakere fra sikkerhetsgruppen og CIKTSO-gruppen[27].

Det er gjennomført ROS i forbindelse med overgang fra lokal drift til skyløsning for kommunens ERP-system (Visma), som vurderer risikomomenter knyttet til blant annet uautorisert tilgang, dataangrep og manglende sikkerhetskopiering, og identifiserer tiltak for hvert risikomoment.[28]

I intervju fremkommer det at IKT-ROS-analysen har behov for revisjon, ettersom risikobildet har endret seg vesentlig siden analysen ble utarbeidet i 2022, særlig knyttet til krig og cyberangrep. Det opplyses at revisjonsarbeidet var igangsatt per februar 2026, og at IKT-ROS-analysen er planlagt revidert i løpet av 2026. Det opplyses videre at den helhetlige kommunale ROS-analysen også skal revideres i 2026, og at scenarioet knyttet til IKT-sikkerhet vil bli oppdatert som del av dette arbeidet.

4.3.3 Beredskapsplanverk

Rana kommune har utarbeidet et hierarkisk beredskapsplanverk for håndtering av IT-hendelser og cyberangrep, strukturert i tre nivåer: overordnet beredskapsplan for kommunen (nivå 1), sektorberedskapsplan for støttetjenesten (nivå 2), samt en egen beredskapsplan for IKT-avdelingen (nivå 3). Sektorberedskapsplanen og IKT-avdelingens beredskapsplan er gjensidig koordinerte og støtter opp under den overordnede beredskapsplanen. Den overordnede beredskapsplanen er omtalt i kapittel 3.3.3.

Beredskapsplan Støttetjenesten 2025-2027

Sektorplanen for støttetjenesten er vedtatt av kommunaldirektør stab 15.10.2025. Støttetjenesten omfatter HR- og organisasjonsavdelingen, økonomiavdelingen, IKT-avdelingen og kommuneadvokat. Planen inneholder roller og ansvar i beredskapsorganiseringen, varslingslister, tiltakskort for 11 hendelser i henhold til overordnet ROS, nødplakat for digitale angrep og referanser til sentrale beredskapsprosedyrer i EQS.

Planen spesifiserer at IKT-sjef er del av beredskapsstaben i støttetjenesten og har ansvar for IT-drift, systemer, arkiv og tilrettelegging av infrastruktur. IKT-sjef er kriseledelsens kontaktpunkt mot IT-leverandører, sikkerhetsmyndigheter og annen spisskompetanse innenfor IKT-drift og -sikkerhet, og iverksetter beredskapsplan IKT ved krise.

Beredskapsplan for IKT-avdelingen

Beredskapsplanen for IKT-avdelingen er vedtatt administrativt 01.10.2024. Planen beskriver hvordan IKT-avdelingen skal organisere og gjennomføre beredskapsarbeidet ved krisesituasjoner, med særlig vekt på å opprettholde kritiske IT-systemer. Det fremgår av planen at IKT-avdelingen har ansvar for å opprettholde IKT-systemer med kritiske funksjoner for liv og helse, samt for at tekniske kommunikasjonslinjer internt i kommunen fungerer under en krise.

Planen inneholder blant annet:

[27] Ledelsens gjennomgang 2024 – informasjonssikkerhet, personvern og IKT-sikkerhet, ID 10204
[28] Risiko og sårbarhetsanalyse – Visma over i sky – Nytt ERP, versjon 2, 18.06.2024

- varslingsprosedyrer for ansatte i tre trinn og for eksterne aktører, herunder driftsleverandør og sikkerhetsmyndigheter,
- organisering av beredskapsstab med åtte definerte roller,
- åtte tiltakskort og hendelseslogger i Rayvn for ulike IT-hendelser, herunder cyberangrep, datasikkerhetsbrudd, serverkrasj og kommunikasjonsbrudd,
- spesifikk prosedyre for håndtering av cyberangrep og ransomware,
- en *Impact/Urgency*-matrise for prioritering av systemer ved krisesituasjoner,
- nødplakat for digitale angrep fra Næringslivets sikkerhetsråd, og
- prosedyrer for kontakt med sikkerhetsmyndigheter.

Planen er supplert med en kontinuitetsplan som angir prioriteringsrekkefølge for systemer og minimumsbemanning ved krisesituasjoner. I intervju fremkommer det at beredskapsplanen er noe omfattende, og at det kan være vanskelig å raskt finne frem til det vesentlige ved en hendelse. Det er igangsatt en revisjon av planen (og som annet skal bidra med forenkling og effektivisering) med mål om ferdigstillelse før sommeren 2026.

4.3.4 Samhandling

Rana kommune er medlem i KINS (Kommunal informasjonssikkerhet) og Helse-CERT, og deltar på samlinger og seminarer i regi av NSM. Helse-CERT gir bistand ved behov, har døgntelefon og responderer raskt på henvendelser. Kommunen abonnerer på varslingsmeldinger om sårbarheter i nettverksutstyr og mottar varsler fra Helse-CERT om lekkede passord, slik at kompromitterte e-postadresser og brukere i ulike systemer raskt kan følges opp.

Kommunen har én hovedleverandør for drift (Braathe), som ivaretar on-premise-infrastruktur og har vaktordning som kan kontaktes ved hendelser. Driftsleverandøren overvåker serversiden og varsler ved unormaliteter. I tillegg benyttes flere SaaS-løsninger, blant annet for sak/arkiv, ERP og helsesystemer. Kommunen har vurdert å anskaffe en SOC-tjeneste (Security Operations Center), men dette er ikke prioritert innenfor gjeldende budsjett.

Kommunen samarbeider med Digitale Helgeland i digitaliseringsprosjekter og benytter personvernombud gjennom Digitale Helgeland. Personvernombudet har bistått kommunen i forbindelse med risikovurderinger, DPIA og databehandleravtaler, og det er planlagt tettere samhandling med Digitale Helgeland ved digitale beredskapshendelser.

I intervju blir det pekt på at det historisk har vært lite fokus på operasjonell teknologi (OT) som en del av kommunens IKT-beredskapsarbeid, men dette er nå løftet opp som et prioritert område. En hendelse knyttet til vann og avløp i løpet av det siste halve året har ført til økt samarbeid med teknisk sektor og bistand fra Helse-CERT. Ledelsens gjennomgang 2024 peker på et stort behov for å kartlegge og kategorisere OT-systemer etter risiko og sårbarhet.

Kommunen deltar i et regionalt samarbeid om beredskap, herunder om innføring av krisestøtteverktøyet Rayvn i samarbeid med nabokommuner og sykehuset. En ny regional beredskapskoordinator for Nord-Helgeland, som startet i oktober 2025, skal samordne kommunene, harmonisere planverk og tilrettelegge for felles øvelser. Kommunen er videre bevisst på at den ikke kan håndtere alle risikoer alene, og har etablert

samarbeidsavtaler med leverandører og aktører som har nødvendig kompetanse innenfor IKT-sikkerhet.

4.3.5 Sikkerhetstiltak og internkontroll

Styringsdokumenter for IKT-sikkerhet

Rana kommune har oversendt 13 overordnede retningslinjer for IKT-sikkerhet. Retningslinjene omfatter et overordnet styringsdokument basert på ISO 27001, samt policyer for blant annet passordkvalitet, bruk av kunstig intelligens, brukerutstyr, fjernarbeid, kryptografi, nettverkssikkerhet, tilgangsstyring, logging, sikkerhetskopiering og gjenoppretting, og kontinuerlig forbedring. I tillegg dekkes personvernrelaterte områder som overføring av personopplysninger og ivaretakelse av registrertes rettigheter. En oversikt over retningslinjene og innholdet i disse fremgår av Tabell 6 (se vedlegg).

I tillegg til de overordnede retningslinjene har kommunen oversendt 15 operative rutiner, prosedyrer og sjekklister som konkretiserer hvordan de overordnede føringene skal implementeres og etterleves i det daglige arbeidet med IKT-sikkerhet. Dokumentene dekker blant annet hendelseshåndtering, avvikshåndtering ved brudd på personopplysningssikkerheten, håndtering av løsepengetrusler, gjennomføring av risikovurderinger og personvernkonsekvensvurderinger (DPIA), tilgangsstyring, sikker konfigurasjon, sårbarhetshåndtering, leverandørstyring og opplæring av ansatte. Oversikt over de oversendte rutinene fremgår av Tabell 7 (se vedlegg).

Status på implementering og etterlevelse

Kommunen har valgt å benytte ISO 27001, ISO 27002 og ISO 27701 som faglige referanserammer for å vurdere modenhet og fremdrift i eget styringssystem for informasjonssikkerhet og personvern. Ledelsens gjennomgang 2024 viser at implementeringen er i en tidlig fase, der flertallet av kontrollene i de aktuelle standardene er delvis implementert eller ikke påbegynt. Sikkerhetsorganisasjonen har i denne fasen prioritert å etablere nødvendige retningslinjer og rutiner, og arbeidet med full implementering og etterlevelse pågår.

Ledelsens gjennomgang dokumenterer at kommunen har iverksatt flere sentrale tekniske sikkerhetstiltak. Tofaktorautentisering er implementert i alle on-premise- og SaaS-applikasjoner, med flerfaktorautentisering gjennom Conditional Access i M365/Azure og tredjefaktor som sperrer tilgang fra enkelte land. Backup tas daglig og lagres i to datasentre, inkludert immutable backup, og sikkerhetskopiering av Office 365 er implementert. [redacted]

Kommunen har iverksatt flere opplærings- og bevissthetstiltak, herunder KS sin kampanje for å hindre dataangrep og digitale hendelser i 2024/2025 og sikkerhetsverktøyet Secure Practice fra januar 2025. Det er også gjennomført flere nettfiskingskampanjer de siste årene som viser varierende resultater. Ledelsens gjennomgang konkluderer med at det er behov for å øke kompetanse og bevissthet rundt personvern og informasjonssikkerhet i hele organisasjonen.

Alle sektorer har egen sikkerhetsorganisering, og kommunen har en dedikert rådgiver for personvern og informasjonssikkerhet samt personvernombud gjennom Digitale

Helgeland. Sikkerhetsgruppen og CIKTSO-gruppen er nærmere beskrevet i kapittel 4.3.1. Ledelsens gjennomgang peker på behov for ytterligere styrking av dedikerte ressurser og konkrete økonomiske rammer, i takt med nye regulatoriske krav, økt tilsynsaktivitet og etterslep på blant annet ROS og DPIA. Sikkerhetsorganisasjonen vurderes å ha mange sårbare roller og begrenset robusthet, med vesentlig kompetanse konsentrert hos få personer.

4.3.6 Evaluering og forbedring

Ledelsens gjennomgang er kommunens sentrale mekanisme for systematisk evaluering av arbeidet med informasjonssikkerhet, personvern og IKT-sikkerhet. Gjennomgangen foretas av kommunedirektørens strategiske ledergruppe (SLG), med deltakelse fra sikkerhetsansvarlig, IKT-sjef og personvernombud. Formålet er å vurdere måloppnåelse, behov for korrigerende tiltak og om internkontrollen er hensiktsmessig og effektiv. Ledelsens gjennomgang for 2024 ble behandlet av SLG 26. juni 2025.

Sikkerhetsgruppen og CIKTSO-gruppen, som er nærmere beskrevet i kapittel 4.3.1, arbeider løpende med forbedring av informasjonssikkerhet og personvern gjennom gjennomgang av avvik og kvalitetsmeldinger, oppfølging av tiltak og videreutvikling av internkontrollsystemet. Identifiserte tiltak fra ledelsens gjennomgang og avvikshåndtering følges opp i kommunens kvalitetssystem EQS med ansvarlig og frister.

Kommunen arbeider med evaluering og forbedring av IKT-beredskap i samsvar med rutiner som er etablert for dette generelt i kommunen (jf. kap. 3.3.4). Kommunen har gjennomført følgende øvelser av relevant for IKT i perioden 2023-2025:

- Øvelse Nordland 2023, 27. januar 2023: Spilløvelse i regi av statsforvalteren i Nordland, med scenario nasjonalt cyberangrep, som medfører stans i nasjonalt transmisjonsnett (420kv), sporadisk utfall av mobilnett, og at Nets betalingsløsninger og BankID er nede.
- IKT-skrivebordsøvelse, 12. oktober 2024[29]: Skrivebordsøvelse med ekstern øvingsleder fra Sikri AS, med scenario inspirert av ransomware-angrepet mot Østre Toten kommune. Øvingsleder vurderte at IKT-avdelingen er dimensjonert for å håndtere slike hendelser, og at kommunen har innført regimer for autentisering, sikkerhetskopiering og gjenoppretting i tråd med myndighetenes anbefalinger.

Dokumentasjonen viser at både spilløvelsen fra 2023 og skrivebordsøvelsen fra 2024 ble evaluert. Evalueringen av Øvelse Nordland 2023 avdekket blant annet utfordringer knyttet til loggføring og bruk av krisestøtteverktøyet CIM, herunder behov for bedre systematikk i tagging av logger, prioriterte ressurser til loggføring og uavklarte prosedyrer for loggføring og samhandling ved strømbrudd. Det ble videre påpekt at gjeldende beredskapsplaner ikke var tilstrekkelig oppdatert for heldigitale tjenester, og at det var behov for klarere retningslinjer ved bortfall av funksjoner som strøm, telekom og ekom. Stab/støtte identifiserte behov for at IKT i samarbeid med tjenesteleverandører kartlegger konsekvenser ved ulike scenarier, særlig for nett- og telefonileverandører, og at det må arbeides videre med backup- og reserveløsninger.

I evalueringen fra skrivebordsøvelsen i 2024 ble identifisert seks forbedringspunkter: behov for økt kunnskap om trusler og tiltak hos IKT-avdelingen og ledelsen, fullstendig

[29] Øvingsrapport Rana kommune – IKT-sikkerhet, oktober 2024

oversikt over systemer og infrastruktur med verdivurdering etter kritikalitet, tydeligere definering av systemansvarliges rolle for skytjenester, gjennomgang av beredskapsplan og rutiner for gjenoppretting, hyppigere øvelser (én til to ganger årlig) også for beredskapsledelsen, og jevnlige kompetansekampanjer rettet mot ansatte. Tiltakene er lagt inn i EQS for oppfølging, og i forbindelse med verifisering opplyser kommunen at flere av forbedringspunktene er fulgt opp. Det er gjennomført kompetansetiltak innen IKT-sikkerhet, herunder bruk av Secure Practice i 2025 og JungleMap i 2026, treningsprogram for alle ansatte med tilgang til kommunens domene, samt samarbeidsavtale med KINS med tilpassede policyer og bruk av opplæringsressurser. IKT-avdelingen deltar videre på informasjons- og læringsmøter innen IKT-sikkerhet.

Beredskapsplanen er under revisjon med mål om ferdigstillelse før sommeren 2026. Det er også igangsatt revisjon av IKT-ROS-analysen per 27. februar 2026. Beredskapsplanen angir at øvelser og gjennomgang av planen skal gjennomføres årlig, med evaluering og rapportering til kommunaldirektør etter hendelser og øvelser. Rana kommune opplyser i verifisering at helhetlig ROS skal revideres i 2026, og at scenario knyttet til IKT-sikkerhet skal revideres.

Kommunen har som ledd i det løpende forbedringsarbeidet iverksatt opplærings- og bevissthetstiltak som er nærmere beskrevet i kapittel 4.3.5. Ledelsens gjennomgang konkluderer med at det er behov for å øke kompetanse og bevissthet rundt personvern og informasjonssikkerhet i hele organisasjonen.

4.3.7 Casegjennomgang: Profil omsorg

Visma Omsorg Profil (heretter «Profil omsorg») er kommunens elektroniske pasientjournalsystem (EPJ) for pleie- og omsorgssektoren. Systemet benyttes innen helse og mestring til blant annet å dokumentere helsehjelp, registrere medisiner, håndtere avvik og kommunisere med samarbeidspartnere via elektroniske meldinger. Systemet inneholder særlige kategorier av personopplysninger, herunder helseopplysninger om et stort antall brukere av kommunens helse- og omsorgstjenester. Systemet driftes av Braathe på vegne av kommunen, og er en SaaS/on-premise-hybridløsning levert av Visma. Systemeier er kommunaldirektør for helse og mestring, og systemadministrator er avdelingsleder for fagutvikling og innovasjon samt rådgiver i helse- og mestringstjenesten.

Systemets betydning og sårbarhet

Profil omsorg er et forretningskritisk system for helse og mestring i Rana kommune. Systemet benyttes av alle tjenestene i helse og mestring, unntatt legetjenesten, og er det primære verktøyet for dokumentasjon av helsehjelp i henhold til helsepersonelloven og pasientjournalforskriften. Systemet inneholder blant annet elektroniske pasientjournaler, medisinkort, diagnoser, avviksmeldinger og elektroniske meldinger til og fra samarbeidspartnere som Helgelandssykehuset og fastleger.

Et cyberangrep mot Profil omsorg – eksempelvis ransomware, datainnbrudd eller tjenestenektangrep – vil kunne få alvorlige konsekvenser for både tjenesteproduksjonen og de registrertes personvern. Bortfall av systemet vil direkte ramme ansattes mulighet til å dokumentere helsehjelp, administrere medisiner og kommunisere med samarbeidspartnere, og vil i ytterste konsekvens utgjøre en risiko for pasientsikkerheten..

I intervju kom det fram at det tidvis har vært utfordringer knyttet til nedetid, i tilfeller der IKT-avdelingen ikke alltid har tatt tilstrekkelig hensyn til at Profil omsorg må være tilgjengelig døgnkontinuerlig, herunder nedetid på kort varsel og vesentlig lengre nedetid enn varslet. Det opplyses at samarbeidet med IKT-avdelingen har bedret seg den senere tiden. Som et beredskapstiltak ved systemnedetid skriver avdelingene jevnlig ut arbeidsplaner og legemiddelkort, for å sikre at medisinering og driftskontinuitet skal kunne ivaretas i forbindelse med oppdatering og vedlikehold av systemet.

Forebyggende tiltak for å motvirke cyberangrep

Tilgangsstyring er et sentralt forebyggende tiltak for Profil omsorg. Det er utarbeidet en egen rutine for opprettelse, endring og avslutning av tilganger i systemet, og alle henvendelser om tilganger skal komme fra nærmeste leder. Tilganger gjennomgås og ryddes systematisk to ganger i året, før og etter ferieavvikling.

Kommunen har videre utarbeidet en detaljert oversikt over tilganger for ulike ansattroller, jf. krav i egen tilgangsstyringsrutine. Tilganger tildeles etter prinsippet om minste nødvendige rettigheter, der den ansattes rolle og tilhørighet avgjør tilgang til moduler, organisasjonsenheter, institusjoner, funksjonsgrupper og tjenestegrupper.

Systemet har et samtykkeregime med mulighet for person- og elementrestriksjoner, som gir brukerne kontroll over hvem som har tilgang til deres journal. Alle oppslag i journalen skal begrunnes og loggføres. **Tofaktor-autentisering** og **sikkerhetskopiering** er implementert som del av kommunens overordnede tekniske sikkerhetstiltak, jf. omtale i 4.3.5. Sikkerhetskopiering ivaretas av driftsleverandøren Braathe.

Opplæring av nyansatte i bruk av Profil omsorg, som også omfatter sikkerhetsopplæring og innføring i sikkerhetskrav (tofaktor-autentisering, påloggingsrutiner mm.), er regulert gjennom sjekkliste for nyansatte og opplæringsmateriell i EQS og DigiPro Helse. Det er leder i den enkelte avdeling som er ansvarlig for opplæringen. Systemadministrator for Profil omsorg viser til at opplæring i stor grad blir gjennomført, men at det likevel forekommer avvik fra ansatte i etterlevelse av kommunens interne krav, som må følges opp.

Beredskap for og håndtering av cyberangrep

Ved en IKT-hendelse som berører Profil omsorg følges kommunens etablerte saksflyt for IKT-henvendelser, der saker meldes inn via Pureservice og håndteres av IKT-avdelingen i samarbeid med driftsleverandøren Braathe og systemleverandøren Visma. Systemadministrator og superbrukere vurderer om saken kan løses lokalt eller må eskaleres. Ved alvorlige IKT-hendelser, herunder ransomware-angrep, følges kommunens rutine for løsepengetrussel, jf. omtale i 4.3.5.

Sjekkliste for ansatte ved mistanke om ransomware gir en enkel handleliste for hva den enkelte ansatte skal gjøre ved tegn på angrep. Dersom et cyberangrep medfører brudd på personopplysningssikkerheten, utløses meldeplikt til Datatilsynet etter GDPR artikkel 33 og eventuell varslingsplikt overfor berørte registrerte, jf. kommunens avvikshåndteringsrutine omtalt i 4.3.5.

Sikkerhetsansvarlig i helse og mestring er kontaktpunkt ved brudd på personopplysningssikkerheten, og vurderer behov for involvering av overordnet

sikkerhetsansvarlig og Datatilsynet. Kommunen har videre etablert kontakt med KommuneCERT og Helse-CERT for bistand ved alvorlige IKT-hendelser, jf. omtale i kap. 4.3.4.

I intervju ble det pekt på flere utfordringer i organiseringen av beredskap knyttet til IKT og cyberangrep. Kommunaldirektør og ansatte i helse og mestring har beredskapsansvar for systemet, uten at de har innsikt i overordnede ROS-analyser eller cyberangrepsscenarioer for de tekniske løsningene systemet er avhengig av. Det kom frem at IKT-avdelingen og helse og mestring har gjennomført risikovurderinger separat, uten noen særskilt samhandling og koordinering av prosessene. Flere intervjuede etterlyser økt samhandling og gjennomføring av risikovurderinger i fellesskap, for å sikre at systemberedskapen er helhetlig og fullstendig oppbygd.

Videre opplever systemadministrator uklare ansvarsforhold mellom IKT-avdelingen og driftsleverandøren Braathe ved innmelding av saker som gjelder Profil omsorg, noe som medfører risiko for forsinket håndtering. Det er utarbeidet en ny rutine for å møte denne utfordringen.

I intervju blir det vist til at det nylig har blitt foretatt et bytte av servere som er knyttet til Profil omsorg. I etterkant av overgangen til nye servere ble det oppdaget at ansatte kunne logge seg på Profil omsorg fra private PC-er via Citrix. Muligheten ble stengt etter noen dager. Det arbeides nå med å etablere oversikt over hvem som skal ha tilgang til systemer med sensitiv informasjon utenfor kommunens nettverk, og hvordan dette skal håndteres for å ivareta nødvendig sikkerhet.

Status på systemspesifikk sikkerhet og beredskap for Profil omsorg

Gjennomgangen av dokumentasjon og intervjuer viser følgende status for systemspesifikk beredskap knyttet til Profil omsorg:

- Det ble i 2010 gjennomført en risiko- og sårbarhetsanalyse (ROS) for elektronisk meldingsutveksling (EMU) via Profil. Analysen omhandler risiko knyttet til utveksling av elektroniske meldinger mellom helse- og sosialavdelingen, omsorgsavdelingen og fastleger via Norsk Helsenett, og identifiserer 18 uønskede hendelser med vurdering av sannsynlighet, konsekvens og forslag til tiltak. Analysen dekker ikke dagens trusselbilde, herunder cyberangrep, ransomware, tjenestenektangrep, datainnbrudd og lekkasje av helseopplysninger, og omhandler ikke systemets avhengigheter av skytjenester og ekstern driftsleverandør. Det foreligger ikke en personvernkonsekvensvurdering (DPIA) for Profil omsorg. Kommunen viser for øvrig til overordnede IKT-ROS-er og NSMs rammeverk.
- Det er ikke utarbeidet et dedikert tiltakskort for bortfall av Profil omsorg, men det foreligger en beredskapsplan for manuell drift og gjenoppretting av systemet. Kommunen har generelle rutiner for ransomware, avvikshåndtering mv., jf. omtale i 4.3.5, men disse er ikke tilpasset det konkrete scenarioet med bortfall av EPJ-systemet i helse og mestring.
- Sikkerhetsorganisasjonen for Profil omsorg er sårbar, med systemkompetansen konsentrert hos få nøkkelpersoner. Systemadministratorer mottar alltid beskjed når ansatte bytter avdeling og skal ha nye tilganger, men varsling om at tilganger skal avsluttes kan glippe, noe som medfører risiko for at tilganger ikke avsluttes i tide. Som

kompenserende tiltak sendes det halvårlig ut lister til avdelingslederne for bekreftelse, og det pågår et prosjekt for automatisk varsling ved onboarding og offboarding.
- Resultatene fra nettfiskingskampanjene, jf. omtale i 4.3.5, viser at en betydelig andel ansatte er sårbare for sosial manipulering.

Det pågår en anskaffelse av nytt felles EPJ-system for kommunene på Helgeland, som forventes ferdigstilt i løpet av sommeren 2026. Kommunen opplyser at det i anskaffelsen er det lagt stor vekt på robuste driftsmiljøer for å redusere sårbarhet knyttet til systemkompetansen. Overgangen vil innebære en periode med endringer i systemlandskapet for helse- og mestringstjenesten, og vil også påvirke dagens sikkerhetsbilde/-situasjon.

4.4 Vurderinger

4.4.1 Roller og ansvar

Kommunen har etablert en sikkerhetsorganisasjon med dedikerte roller og faste møtestrukturer. Tverrsektoriell samordning gjennom sikkerhetsgruppen og CIKTSO-gruppen, og sikkerhetsorganisering i alle sektorer, bidrar til å oppfylle kravet om å kartlegge roller og ansvar for IKT-sikkerhet internt i virksomheten, jf. kommuneloven § 25-1 og NSM grunnprinsipp 1.3.

Ansvarsfordelingen mellom IKT-avdelingen, fagmiljøene i sektorene og eksterne leverandører er ikke tilstrekkelig tydelig kartlagt på alle områder. Det har vært uklarheter i ansvarsforholdet mellom IKT-avdelingen, driftsleverandør og systemeiere i sektorene, og risikovurderinger har vært gjennomført separat uten tilstrekkelig samhandling. Dette er ikke i samsvar med kravet om at roller og ansvar for IKT-sikkerhet kartlegges også hos eksterne leverandører og partnere, og at det klargjøres hvem som skal kontaktes ved hendelser, jf. NSM grunnprinsipp 1.3. Deloitte merker seg at det opplyses om at det er etablert månedlige møter mellom IKT-avdelingen og Helse og Mestring som et tiltak for å forbedre samhandlingen knyttet til systemet Profil omsorg[30].

Sikkerhetsorganisasjonen opplyses å ha flere sårbare roller og begrenset robusthet, med vesentlig kompetanse konsentrert hos få personer. Dette gjør arbeidet med IKT-sikkerhet personavhengig, og utgjør en risiko for kommunens evne til å opprettholde et forsvarlig sikkerhetsnivå over tid (f.eks. ved skifte av nøkkelpersonell). Det gjenstår følgelig arbeid med å sikre tilstrekkelig robusthet gjennom kompetanseoverføring og stedfortrederfunksjoner, jf. forskrift om kommunal beredskapsplikt § 4 c og NSM grunnprinsipp 1.3.

4.4.2 Risiko- og sårbarhetsanalyser knyttet til cyberangrep

Rana kommune har gjennomført en egen IKT-ROS strukturert etter NSMs grunnprinsipper, som dekker sentrale risikokategorier med vurdering av sannsynlighet, konsekvens og eksisterende tiltak. IKT-ROS-en er videre koblet til kommunens helhetlige ROS, som inkluderer digitale trusler som eget scenario, jf. 3.4.2. Etter Deloittes vurdering

[30] I forbindelse med verifisering opplyser Rana kommune at overgangen fra lokal servertjeneste til eksternt tjenestekjøp i 2025 har medført en overgangsfase med endring av rutiner og samhandling etter hvert som de ulike fagsystemene har blitt flyttet over.

bidrar dette til at IKT-sikkerhetsrisiko ses i sammenheng med kommunens øvrige risikobilde, i tråd med sivilbeskyttelsesloven § 14 og forskrift om kommunal beredskapsplikt § 2.

Det foreligger ikke en oppdatert systemspesifikk ROS eller DPIA for Profil omsorg som omhandler IT-trusler mot systemet, herunder ransomware, datainnbrudd, tjenestenektangrep og lekkasje av helseopplysninger, jf. 4.3.7. Den eksisterende ROS-analysen fra 2010 omhandler elektronisk meldingsutveksling via Norsk Helsenett, men er ikke oppdatert eller dekkende for dagens trusselbilde. Overordnede IKT-ROS-er og NSMs rammeverk ivaretar ikke kravet om at risikovurderingene skal beskrive det enkelte systems betydning for tjenesteleveransen, tilknyttede sårbarheter og konsekvenser, samt avhengighet av andre virksomheter, jf. forskrift om kommunal beredskapsplikt § 2 og NSM grunnprinsipp 1.1.

Ledelsens gjennomgang 2024 dokumenterer videre et vedvarende etterslep av ROS- og DPIA-vurderinger, særlig ved anskaffelse av nye IKT-systemer (jf. kapittel 4.3.2). Fraværet av systemspesifikke risikovurderinger innebærer at kommunen mangler et tilstrekkelig grunnlag for å identifisere og prioritere sikkerhetstiltak for sine mest kritiske informasjonssystemer.

Videre fremkommer det at det er behov for revisjon av IKT-ROS-analysen for å sikre at denne hensyntar endringer i risikobildet for IKT. Arbeidet med revisjon av IKT-ROS-analysen er iverksatt per februar 2026. Deloitte vil peke på at det er viktig at den reviderte analysen også omfatter systemspesifikke risikovurderinger for forretningskritiske systemer, og at analysene oppdateres i takt med endringer i risikobildet, jf. forskrift om kommunal beredskapsplikt § 6.

4.4.3 Beredskapsplanverk

Kommunen oppfyller i hovedsak kravet om en overordnet beredskapsplan som integrerer planer for håndtering av digitale hendelser og cyberangrep, jf. forskrift om kommunal beredskapsplikt § 4 og NSM grunnprinsipp 4.1 og 4.3. Beredskapsplanen for IKT-avdelingen inneholder tiltakskort for ulike IT-hendelser, varslingsprosedyrer og definerte roller, og sektorplanen for støttetjenesten sikrer sammenhengen med det overordnede beredskapsplanverket.

Det foreligger imidlertid ikke et dedikert tiltakskort tilpasset bortfall av Profil omsorg. Det finnes en beredskapsplan for manuell drift og gjenoppretting av systemet, men denne er ikke tilpasset det konkrete scenarioet med bortfall av EPJ-systemet i helse og mestring, jf. kap. 4.3.7. Kravet om prosedyrer for å opprettholde drift ved bortfall av digitale løsninger, inkludert reserveløsninger, jf. sivilbeskyttelsesloven § 15 og NSM grunnprinsipp 4.1 og 4.3, er etter Deloittes vurdering dermed ikke fullt ut oppfylt.

Beredskapsplanverket adresserer i begrenset grad sammenhengen mellom IKT-avdelingens planer og fagmiljøenes behov. Ansatte med beredskapsansvar for forretningskritiske systemer mangler innsikt i overordnede ROS-analyser og cyberangrepsscenarioer, noe som svekker grunnlaget for tilpassede beredskapsplaner og tiltakskort.

Beredskapsplanen for IKT-avdelingen, som inneholder tiltakskortene for cyberangrep og øvrige IT-hendelser, er plassert på nivå 3 i kommunens beredskapsplanverk – det vil si på avdelingsnivå. Cyberangrep er imidlertid en organisasjonsomfattende trussel som kan ramme hele kommunens tjenesteproduksjon, herunder forretningskritiske systemer som Profil omsorg, jf. kap. 4.3.7. NSMs grunnprinsipper understreker at toppledelsen må ta eierskap til og involvere seg i sikkerhetsarbeidet, og at styringsstrukturer, ansvar og rapporteringslinjer må være etablert på tvers av organisasjonen, jf. NSM grunnprinsipp 1.1 og 4.1. Deloitte vurderer at plasseringen av det operative cyberangrepsplanverket primært på avdelingsnivå innebærer en risiko for at alvorlige digitale hendelser ikke i tilstrekkelig grad forankres og koordineres på overordnet ledelsesnivå, og at dette bør vurderes i forbindelse med den pågående revisjonen av beredskapsplanen.

4.4.4 Samhandling

Kommunen har etablert ulike former og tiltak for samarbeid med relevante eksterne aktører når det gjelder forebygging av og beredskap mot cyberangrep, herunder fast kontakt og samarbeid med KommuneCERT og Helse-CERT for bistand ved alvorlige IKT-hendelser, deltakelse på samlinger og seminarer med NSM, prosedyrer for varsling til og samhandling med driftsleverandør av de ulike systemene kommunen benytter osv. Deloitte vurderer at kommunen gjennom de samarbeidsformene og -tiltakene som er implementert, har ivaretatt kravet om varslingsliste over aktører med roller i krisehåndtering av cyberhendelser, jf. forskrift om kommunal beredskapsplikt § 4 og NSM grunnprinsipp 4.1, samt i stor grad ivaretar sitt ansvar etter samvirkeprinsippet.

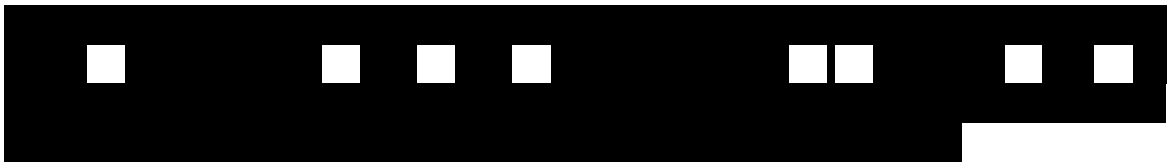
I casegjennomgangen av Profil omsorg er det samtidig påpekt noen utfordringer i samhandlingen på operativt nivå. Systemadministrator for Profil omsorg opplever uklare ansvarsforhold mellom IKT-avdelingen og driftsleverandøren Braathe ved innmelding av saker, og ansatte med beredskapsansvar for forretningskritiske systemer mangler innsikt i overordnede ROS-analyser og cyberangrepsscenarioer. Dette svekker etter Deloittes vurdering forutsetningene for effektiv samhandling under håndtering av et cyberangrep, og bør følges opp for å sikre at nødvendig samhandling fungerer som tiltenkt ved denne type hendelser.

4.4.5 Sikkerhetstiltak og internkontroll

Kommunen har etablert et rammeverk med overordnede retningslinjer og operative rutiner som dekker sentrale områder for IKT- og informasjonssikkerhet, og har etter Deloittes vurdering iverksatt relevante teknologiske sikkerhetstiltak jf. NSM grunnprinsipp 2.2, 2.4, 2.6, 2.9 og 3.2. Deloitte merker seg også at kommunen arbeider kontinuerlig med å teste og forbedrer sikkerheten, i samsvar med krav i forskrift om kommunal beredskapsplikt § 8 og NSM grunnprinsipp 4.3.

Samtidig viser gjennomgangen at ikke alle retningslinjer og rutiner er fullt ut implementert og etterlevd. [redacted]

Nedenfor oppsummeres og vurderes internkontrollen på de ulike hovedtiltaksområdene:

- **Innlogging og sikkerhet**: Tofaktorautentisering er implementert i alle on-premise- og SaaS-applikasjoner, med flerfaktorautentisering gjennom Conditional Access i M365/Azure og passordpolicy med krav om minimum 14 tegn. Kravene til sterk autentisering er i vesentlig grad oppfylt, jf. NSM grunnprinsipp 2.6. Hendelsen der ansatte etter serverovergang kunne logge seg på Profil omsorg fra private PC-er via Citrix, jf. 4.3.7, illustrerer imidlertid at sikkerhetskonfigurasjonen er sårbar ved endringer i driftsmiljøet.
- **Tilgangsstyring**: Kommunen har overordnede retningslinjer for tilgangsstyring, men IKT-sjefen opplyser at offboarding ikke er fullt ut på plass og at gjennomganger av brukertilganger ikke skjer etter faste intervaller. For Profil omsorg er det etablert detaljert tilgangsoversikt med rollebasert tilgangskontroll, halvårlig gjennomgang og logging av alle oppslag, jf. 4.3.7. Systemadministratorer mottar alltid beskjed når ansatte bytter avdeling og skal ha nye tilganger, men varsling om at tilganger skal avsluttes kan glippe, noe som medfører risiko for at tilganger ikke avsluttes i tide, jf. 4.3.7. Kravet til tilgangsstyring er delvis oppfylt, jf. NSM grunnprinsipp 2.4.
- 
- **Sikkerhetskopi og gjenoppretting**: Backup tas daglig og lagres i to datasentre, inkludert immutable backup, og sikkerhetskopiering av Office 365 er implementer. Skrivebordsøvelsen i oktober 2024 bekreftet at kommunen har innført regimer i tråd med myndighetenes anbefalinger, jf. 4.3.6. Kravet er oppfylt, jf. NSM grunnprinsipp 2.9 og 3.2.
- **Opplæring av ansatte**: Kommunen har iverksatt relevante tiltak, herunder KS-kampanjen og Secure Practice. Resultatene fra nettfiskingskampanjene viser imidlertid at en betydelig andel ansatte er sårbare for sosial manipulering. Kravet om opplæringssystem som sikrer nødvendige kvalifikasjoner er delvis oppfylt, jf. forskrift om kommunal beredskapsplikt §§ 1 og 4 c og NSM grunnprinsipp 1.3.
- **Overvåking og varsling**: Driftsleverandøren Braathe overvåker serversiden og varsler ved unormaliteter, kommunen har etablert ISMS-dashboard, abonnerer på varslingsmeldinger fra Helse-CERT og har døgnkontinuerlig vaktordning i IKT-avdelingen. Kommunen har vurdert, men ikke prioritert å investere i en SOC-tjeneste for døgnkontinuerlig sikkerhetsovervåking. Deloitte vurderer at kommunen gjennom de etablerte tiltakene har et bevisst forhold til risikoen og har iverksatt hensiktsmessige tiltak for overvåking og varsling, jf. NSM grunnprinsipp 3.2.

Samlet sett vurderer Deloitte at kommunen har iverksatt hensiktsmessige internkontrolltiltak på flere sentrale deler av IKT-sikkerhetsområdet, særlig knyttet til autentisering, tilgangsstyring, sikkerhetskopiering og overvåking. Samtidig er det Deloittes vurdering at kommunen for å sikre en hensiktsmessig internkontroll på alle de ovenstående områdene, må jobbe videre med å styrke opplæringstiltak blant ansatte.

4.4.6 Evaluering og forbedring

Etter Deloittes vurdering bidrar ledelsens gjennomgang til å oppfylle kravet om systematisk evaluering og forbedring av beredskapsplanverket, jf. forskrift om kommunal beredskapsplikt § 6 og kommuneloven § 25-1. Gjennomgangen gir en systematisk

evalueringsstruktur der kommunedirektørens strategiske ledergruppe årlig vurderer måloppnåelse, behov for korrigerende tiltak og internkontrollens hensiktsmessighet. Kommunen har videre etablert hensiktsmessige kanaler for å holde seg oppdatert på nye digitale trusler gjennom deltakelse i relevante nettverk, jf. NSM grunnprinsipp 4.3.

IKT-avdelingen gjennomførte i oktober 2024 en skrivebordsøvelse som ble evaluert, og som resulterte i seks konkrete forbedringspunkter som er lagt inn i EQS for oppfølging. Opplærings- og bevissthetstiltakene knyttet til IKT-sikkerhet er videre evaluert som del av ledelsens gjennomgang 2024. Etter Deloittes vurdering har kommunen dermed etablert en praksis for evaluering av gjennomførte øvelser og tiltak på IKT-sikkerhetsområdet, i tråd med forskrift om kommunal beredskapsplikt § 8 og NSM grunnprinsipp 4.3.

4.4.7 Casegjennomgang: Profil omsorg

Casegjennomgangen av beredskap for cyberangrep mot Profil viser at Rana kommune har iverksatt relevante sikkerhetstiltak for systemet som etter Deloittes vurdering bidrar godt til å motvirke negative konsekvenser av cyberangrep, herunder blant annet detaljert tilgangsstyring med rollebasert tilgangskontroll, tofaktorautentisering, sikkerhetskopiering av data og fysisk back-up i tilfelle systemnedetid, samt opplæring av nyansatte i blant annet systemsikkerhet.

Samtidig avdekker gjennomgangen flere forhold som etter Deloittes vurdering ikke er i samsvar med gjeldende krav. Det foreligger ikke en oppdatert systemspesifikk ROS-analyse eller DPIA for Profil omsorg, jf. forskrift om kommunal beredskapsplikt § 2 og NSM grunnprinsipp 1.1. Det er heller ikke etablert et dedikert tiltakskort for bortfall av systemet, jf. sivilbeskyttelsesloven § 15 og NSM grunnprinsipp 4.1 og 4.3. Ansatte med beredskapsansvar for systemet mangler innsikt i overordnede ROS-analyser og cyberangrepsscenarioer for IKT-området, noe som svekker forutsetningene for en helhetlig systemberedskap, jf. NSM grunnprinsipp 1.3 og 4.1. Det er videre påvist svakheter i samhandlingen mellom fagmiljøet i helse og mestring, IKT-avdelingen og driftsleverandøren Braathe, samt avvik i ansattes etterlevelse av sikkerhetskrav, jf. NSM grunnprinsipp 1.3 og 2.6. Samlet sett medfører disse forholdene etter Deloittes vurdering risiko for at risikoer og sårbarheter knyttet til Profil omsorg ikke er tilstrekkelig kartlagt, og at det kan mangle tiltak som er nødvendige for å sikre en tilfredsstillende systemspesifikk beredskap for håndtering av cyberangrep mot systemet.

5 Ødeleggelse av kritiske veier

5.1 Problemstilling

I dette kapittelet vil vi svare på følgende hovedproblemstilling med underproblemstillinger:

3. **Har Rana kommune etablert tilstrekkelig beredskap for håndtering av naturhendelse som fører til ødeleggelse av kritiske veier[31]?**
   a) Er roller og ansvar tydelig definert og kommunisert?
   b) Har kommunen gjennomført og dokumentert risiko- og sårbarhetsanalyser som spesifikt omfatter ødeleggelse av kritiske veier?
   c) Foreligger det beredskapsplaner for sykehjem som omtaler ødeleggelse av kritiske veier, og er disse tilstrekkelig detaljerte, oppdaterte og kjent blant relevante ansatte?
   d) Har det blitt gjennomført tilstrekkelig opplæring og øvelser for relevant personell som omfatter ødeleggelse av kritiske veier, og involverer disse alle relevante aktører?
   e) Har kommunen etablert rutiner for systematisk evaluering og oppfølging av beredskapsplaner etter øvelser og hendelser, og blir forbedringspunkter implementert?
   f) Er det utarbeidet tilstrekkelige rutiner og planer for å sikre etterlevelse av samvirkeprinsippet ved ødeleggelse av kritiske veier?

5.2 Revisjonskriterier

Revisjonskriteriene er hentet fra sivilbeskyttelsesloven, forskrift om kommunal beredskapsplikt, vegloven, veidata- og trafikkinformasjonsforskriften og veileder til forskrift om kommunal beredskapsplikt.

Tabell 5: Revisjonskriterier knyttet til scenarioet ødeleggelse av kritiske veier

Tema	Revisjonskriterier (kommunen skal)	Kilde
Risiko- og sårbarhetsanalyser	Kartlegge uønskede hendelser som kan inntreffe i kommunen, herunder naturhendelser som kan føre til bortfall av kritisk vei, vurdere sannsynligheten for at disse inntreffer, og hvordan de kan påvirke kommunen, og sammenstille dette i en helhetlig risiko- og sårbarhetsanalyse (ROS). Kommunal veimyndighet skal gjennomføre jevnlige risiko- og	Sivilbeskyttelsesloven § 14; forskrift om kommunal beredskapsplikt § 2; veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav e

[31] Kritiske veier forstås her som veiforbindelser som er avgjørende for tilgang til og fra viktige samfunnsfunksjoner, som helse- og omsorgsinstitusjoner, nødetater, forsyningslinjer, samt evakuering av innbyggere.

	sårbarhetsanalyser som grunnlag for trafikkberedskapsplaner og omkjøringsruter for kommunale veier, inkludert sårbarhet for naturfare og værrelaterte farer.	
Risiko- og sårbarhetsanalyser; Beredskapsplaner	Utarbeide langsiktige mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhets- og beredskapsarbeidet med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen, herunder for scenario som kan føre til bortfall av kritisk vei.	Forskrift om kommunal beredskapsplikt § 3
Roller og ansvar; Beredskapsplaner; Kapasitet og kompetanse; Samhandling og samarbeid	Kommunal veimyndighet skal kategorisere sitt veinett og avklare behovet for trafikkberedskapsplaner, utarbeide trafikkberedskapsplaner for aktuelle veistrekninger i samråd med andre veimyndigheter der deres veinett blir berørt, innhente nødvendige vedtak for midlertidige trafikkreguleringer, formidle trafikkberedskapsplanene til Nasjonal veidatabank, og utføre sine oppgaver i henhold til trafikkberedskapsplan ved iverksetting av planen. Det bør videre utarbeides temavise beredskapsplaner for veistrekninger som er særlig utsatt for naturfare og uvær, basert på gjennomførte risiko- og sårbarhetsanalyser, med tydelig angivelse av ansvar og frister for utarbeidelse.	Vegloven § 10; veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav b til d, f og g [32]
Roller og ansvar; Samhandling og samarbeid	Ha et selvstendig ansvar for samfunnstrygghet og beredskap for kommunal vei, herunder trafikkberedskap på eget veinett, og samarbeide med øvrige veimyndigheter om trafikkberedskap, omkjøringsruter og stengningslenker.	Vegloven § 10; veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav a, §§ 14-1 og 14-2
Samhandling og samarbeid	Etablere samarbeid med andre relevante aktører om lokale og regionale løsninger av forebyggende og beredskapsmessige oppgaver, med sikte på best mulig utnyttelse av de samlede ressursene, der dette er hensiktsmessig. Samarbeidet bør omfatte veimyndigheter, nødetater og driftsentreprenører med ansvar for trafikkberedskap. Kommunal veimyndighet skal utarbeide	Forskrift om kommunal beredskapsplikt § 5; veileder til forskrift om kommunal beredskapsplikt, kapittel 2.3; veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav c og § 14-2

[32] For mer informasjon, se også Prop. 79 L (2018–2019) kap. 9.1.

	trafikkberedskapsplaner i samråd med andre veimyndigheter der deres veinett blir berørt.	
Beredskapsøvelser og læring; Samhandling og samarbeid	Kommunen skal ha et system for opplæring som sikrer at ansatte med roller i kommunens krisehåndtering har tilstrekkelige kvalifikasjoner. Kommunen skal samarbeide med andre kommuner, veimyndigheter og relevante aktører i øvelser når scenario og øvelsesform tilsier det.	Forskrift om kommunal beredskapsplikt § 7; Veidata- og trafikkinformasjonsforskriften § 14-2
Beredskapsøvelser og læring; Risiko- og sårbarhetsanalyser; Beredskapsplaner	Evaluere krisehåndteringen etter gjennomførte øvelser og uønskede hendelser, herunder hendelser knyttet til bortfall av kritisk vei, og gjøre nødvendige endringer i risiko- og sårbarhetsanalysen og beredskapsplanene basert på evalueringene.	Forskrift om kommunal beredskapsplikt § 8

Se vedlegg 3 for utfyllende revisjonskriterier.

5.3 Datagrunnlag

Den overordnede beredskapsplanen til Rana kommune beskriver de samfunnskritiske funksjoner som kommunen må opprettholde for å dekke innbyggernes grunnleggende behov.[33] Ødeleggelsen av en kritisk vei grunnet en naturhendelse vil true den samfunnskritiske funksjonen «fremkommelighet og transport», og påvirke leveransen av flere samfunnskritiske funksjoner, herunder forsyning av mat og medisiner, drivstoff og energi, nødvendige helse- og omsorgstjenester, kritiske velferdstjenester, og nød- og redningstjeneste. Ved en sammensatt hendelse kan bortfall av kritisk vei forsterke risiko på andre områder.

Mye av kommunens generelle samfunnssikkerhets- og beredskapsarbeid vil være relevant for å håndtere bortfall av kritisk vei. I dette kapittelet vil det i det videre først og fremst vises til dokumentasjon og intervju der bortfall av kritisk vei er omtalt spesifikt. Det vil også vises til det generelle beredskapsarbeidet der det er vurdert som relevant.

5.3.1 Roller og ansvar ved naturhendelser som fører til bortfall av kritisk vei

Rolle- og ansvarsfordelingen overordnet i kommunen er omtalt i kapittel 3. I beredskapsplanen for teknisk sektor, som har ansvar for kommunal vei, går det fram at hendelser håndteres i kommunens linjeorganisasjon med tilhørende fagansvar, der hver sektor har særskilt ansvar for å ivareta lovkrav i egne fagområder, samt for opplæring, øvelser og stabsarbeid. I sektorplanen går det videre fram at organiseringen er basert på prinsippene nærhet, likhet, ansvar og samvirke.[34]

[33] Rana kommune. *Overordnet beredskapsplan Rana kommune*. Vedtatt SLG 26.08.2024.
[34] Rana kommune. *Sektorplan beredskap for tekniske tjenester 2024-2027 Rana kommune*. Vedtatt av kommunaldirektør tekniske tjenester 20.9.2024.

Teknisk sektor består av avdelingene bydrift, areal og miljø og byggdrift, og har beredskapsansvar knyttet til planmyndighet og byggesaksmyndighet, forvaltning av kritisk infrastruktur og brann- og redningstjenesten. Veimyndigheten for kommunale veier er delegert til avdelingssjef bydrift og seksjonsleder for samferdsel. Seksjonslederne innenfor bydrift inngår i kriseledelsen under innsatsleder og operasjon i henhold til sektorberedskapsplanen.

Sektorberedskapsplanen inneholder tiltakskort for 11 hendelser i henhold til RanaROS, som angir hvilke oppgaver de tre avdelingene skal utføre ved den enkelte hendelse. Planen angir videre støttetjenester som sektoren kan tilby, herunder teknisk utstyr med bemanning, brann- og redningstjenester og kommunikasjon via nødnett og satellittelefon. Beredskapsplanen inneholder også en varslingsliste med navngitte personer, roller og telefonnumre. For bydrift foreligger i tillegg en egen varslingsplan som i detalj forklarer hvordan og til hvem den som først får kjennskap til en hendelse innenfor tjenestens ansvarsområde skal varsle, og videre prosess helt opp til kommunaldirektør.

Kommunaldirektør for tekniske tjenester er del av KKL, med avdelingssjef bydrift som stedfortreder. Kommunaldirektøren har i krise fullmakt til å disponere alle ressurser i de tekniske tjenestene etter vanlig driftslinje, og kan delegere tilsvarende fullmakter til sine avdelingssjefer.

Beredskapsstab for teknisk sektor settes når kommunaldirektøren beslutter det. Sammensetningen angis ikke på forhånd, men avgjøres av behovet i den aktuelle situasjonen. Staben driftes etter enhetlig ledelsessystem. Av overordnet beredskapsplan går det fram at KKL kan sammenkalles ved bortfall av kritisk vei, men beredskapsstab på sektornivå kan også settes uten KKL dersom det vurderes at hendelsen kan løses på lavere nivå. I intervju peker flere på at hendelser i stor grad håndteres i linjen, og at KKL sjeldnere settes enn i andre kommuner, herunder også når det gjelder hendelser på det kommunale veinettet.

Brannsjefen er teknisk sektors beredskapskoordinator og hovedansvarlig for beredskap i sektoren. Beredskapskoordinatoren har ansvar for å sikre etterlevelse av lovkrav i egne fagområder, gjennomføre opplæring og øvelser, støtte loggføring og stabsarbeid via krisestøtteverktøyet Rayvn, og forvalte sektorplaner underlagt overordnet planverk.

Både i dokumentasjonen og i intervju vises det til at brann- og redningstjenesten er en viktig aktør i beredskapsarbeidet til Rana kommune. Brann- og redningstjenesten er organisert i to enheter: beredskap og forebyggende. Beredskapsenheten har 25 ansatte i kontinuerlig vaktberedskap og kan innen 15 minutter stille med 12–14 brannkonstabler, i tillegg til 30 brannpersonell med tilgjengelighetsavtale. Tjenesten disponerer en betydelig maskinpark, med nødnettsradioer i alle kjøretøy. Brann- og redningstjenesten har avtaler om å gi bistand til nabokommunene Hemnes, Nesna, Lurøy og Rødøy, samarbeidsavtaler med Mo Industripark (MIP) sikkerhetssenter, flyplassen og redningstjenesten i Storuman kommune i Sverige. I tillegg kan kommunen ved behov rekvirere utstyr og mannskap fra Sivilforsvaret.

5.3.2 Risiko- og sårbarhetsanalyser knyttet til ødeleggelse av kritiske veier

Kommunens helhetlige risiko- og sårbarhetsanalyse er omtalt i kap. 3.3.2. Av de elleve scenarioene som er vurdert og analysert i den helhetlige ROS, er scenario 1 «Ekstremvær og langvarig strømbrudd samt isolering av bygd» særlig relevant for dette kapittelet.[35] I dette scenarioet blir 150 mennesker isolert i 3–4 døgn i en dal i kommunen grunnet et snøskred, og strømmen er brutt. Sårbarhetsvurderingen viser at elleve av DSBs tretten kritiske samfunnsfunksjoner kan bli berørt i dette scenariet. Det konkluderes med at kommunen vil være i stand til å gjenopprette normalsituasjonen relativt raskt, med bistand fra eksterne aktører. Scenarioet er prioritert som det mest kritiske i helhetlig ROS, og i intervju ble det opplyst at scenarioet ble prioritert som nummer én i helhetlig ROS fordi kommunen ofte opplever ekstremværhendelser, og at klimaendringer dessuten øker risikoen for slike hendelser.

Scenarioet omhandler én spesifikk dal i kommunen. Det er gjort en kort vurdering av scenariets overførbarhet til andre steder, samt en kort vurdering av mulige andre hendelser med lignende konsekvenser. På bakgrunn av dette, konkluderes det i helhetlig ROS med at analysen og foreslåtte risikoreduserende tiltak er overførbare til andre geografiske områder og hendelser med lignende konsekvenser. Dette gjelder blant annet tiltak knyttet til beredskapsplanverk, varsling, evakuering, krisekommunikasjon og samhandling med eksterne aktører.

I intervju pekes det samtidig på at konsekvensene av bortfall av en vei varierer betydelig avhengig av hvilken vei det gjelder. Bortfall av en vei inn i en dal med få beboere er ikke nødvendigvis en stor krise, mens bortfall av en hovedferdselsåre er et langt mer alvorlig scenario. Det pekes videre på at ROS-analysen tar utgangspunkt i «worst case»-scenarioer, men at konsekvensene i praksis ofte blir mindre enn fryktet, og at håndteringen av faktiske hendelser i stor grad derfor også må baseres på lokalkunnskap og erfaring relevant for de forholdene som inntreffer.

De foreslåtte tiltakene i helhetlig ROS er listet i statusoversikten over oppfølging av beredskapstiltak, med ansvarlige og status for 2023, 2024 og 2025. Denne listen er gjennomgått i ledelsens gjennomgang i november 2025. Enkelte tiltak er presentert med status «ingen ny status» i 2025, og for noen tiltak viser en tidligere status til DSBcim (DSBs verktøy for informasjonsdeling i forbindelse med ulykker og uønskede hendelser), som ikke lenger er i bruk i kommunen. Ifølge beredskapskoordinator i intervju skyldes dette at noen tiltak ble identifisert før kvalitetssystemet EQS var på plass, og at statusfeltet ikke er oppdatert, selv om tiltakene er gjennomført.

Risikovurderinger for brann og redning

Det er utarbeidet en «Plan for brann og redning» i Rana kommune, der oppdaterte ROSer, beredskapsvurderinger og forebyggende strategier er samordnet og utgjør grunnlag for en handlingsplan for brann- og redningstjenesten. Brann og redningstjenesten har videre utarbeidet en egen risiko- og sårbarhetsanalyse fra 2025. Denne ROSen inneholder beskrivelse av relevante forhold i og utenfor kommunen, vurderinger av tap av kritiske samfunnsfunksjoner, 21 uønskede hendelser som kan inntreffe og sårbarhet,

[35] Rana kommune. *Helhetlig risiko- og sårbarhetsanalyse RanaROS 2022-2025*. Vedtatt av Kommunestyret 10.11.2022 sak 116/22.

sannsynlighet, konsekvenser og usikkerhet for hver av hendelsene. Behov for evakuering er vurdert i alle hendelsene og befolkningsvarsling i noen. Det er presisert at ROS skal oppdateres ved endringer i risikobildet.

I ROS for brann og redning er ekstremvær og brudd på viktig veiforbindelse nevnt som en særskilt sårbarhet for Rana kommune. Vurderingen er begrunnet i prognoser om klimaendringer og historiske erfaringer med ekstremvær i kommunen. Kommunaldirektør for teknisk sektor påpeker i intervju at Rana kommune har over 300 km med vei, som vurderes å være mye for en kommune på Rana sin størrelse.

I tillegg til å være vurdert som en generell sårbarhet for kommunen, handler én av de 21 spesifikke gjennomgåtte hendelsene vurdert i ROS for brann og redning om ekstremvær. Scenarioet vurderes som meget sannsynlig, usikkerheten som moderat og konsekvensene som i snitt noe under middels.

5.3.3 Beredskapsplaner for håndtering av ødelagte veier

Sektor for tekniske tjenester har utarbeidet en egen beredskapsplan som blant annet omtaler roller, ansvar, kommunikasjon, rapportering, økonomi, opplæring, øvelser og evaluering av beredskapsarbeidet i sektoren. Videre inneholder beredskapsplanen tiltakskort for de elleve hendelsene som ble omtalt i helhetlig ROS (jf. kapittel 3.3.2). Tiltakskortet for hendelse 1 «*Ekstremvær, isolert bygd*» angir følgende oppgaver for de tre avdelingene i sektoren:

- **Bydrift**: Stiller nødvendig maskinelt utstyr og mannskap til disposisjon etter bestilling fra kriseledelsen (se mannskaps og utstyrsliste). Kan også rekvirere eksterne ressurser. Avdelingssjef Bydrift kommuniserer med kriseledelsen og egne ressurser via nødnett.
- **Byggdrift:** Hvis det er relevant stilles kommunale bygg til disposisjon med teknisk bistand. Overvåke og sikre kommunale bygg.
- **Areal og miljø**: Kan levere oversikt over hvor mange som er berørt, alderssammensetning og eiere/festere i området. Kan også levere kartdata og kartanalyse.

Sektorberedskapsplanen angir at bydrift har ansvar for drift og vedlikehold av 300 km kommunale veier, og at seksjon samferdsel har 19 fagarbeidere, hvorav de fleste har førerkort for både maskin og klasse C, samt 3 administrative arbeidere. Sektoren disponerer en betydelig maskinpark, herunder veghøvel, hjullastere, hjulgravere, traktorer, lastebiler, skilt- og sperremateriell, strømaggregater og nødnettsradioer. Avdelingssjef bydrift disponerer også en satellittelefon. I vinterhalvåret har kommunen løpende brøytekontrakter med om lag 25 private kontraktører som kan kalles ut på kort varsel. Sektorberedskapsplanen inneholder videre en detaljert oversikt over statlig, fylkeskommunalt og kommunalt veinett i Rana kommune.

Beredskapsplanen for teknisk sektor omtaler hva avdeling for bydrift skal gjøre ved en hendelse som fører til stenging av vei, hvordan en slik hendelse skal håndteres i praksis, intern og ekstern samhandling eller hva slags informasjon som skal gis til hvem og på hvilke tidspunkt. Det er heller ikke utarbeidet annet planverk i kommunen som omtaler noen av de nevnte forholdene. Rana kommune har ikke utarbeidet prosedyrer for

trafikkberedskap, omkjøringsruter eller stengningslenker for kommunale veier[36]. Kommunen opplyser at den forholder seg til overordnet ROS og NVEs faresonekart.

I intervju beskrives håndtering av bortfall av kritisk vei beskrives som i stor grad basert på lokalkunnskap og erfaring fremfor formaliserte trafikkberedskapsplaner. Det pekes på at ved for eksempel en brokollaps vil kommunen etablere fysiske sperringer og kontakte deretter Statens vegvesen. Vegvesenet videreformidler informasjonen til Forsvaret, som har lager med reservebroer. Denne samhandlingen er ikke formalisert i beredskapsplanverket.

Sektorplanen for helse og mestring vurderer ikke konsekvensene av bortfall av kritiske veier for sektorens tjenester. Sektorplanen inneholder syv ROS-analyser – for henholdsvis utfall av EKOM, legemiddelmangel, forsyningssvikt av smittevernutstyr, bortfall av strøm, svikt i vannforsyning, brann i kommunal institusjon og bortfall av arbeidskraft – men ingen av disse omhandler stengte veistrekninger som årsak til eller forverrende faktor ved en hendelse. Sektorplanen omtaler heller ikke hvordan hjemmetjenestene skal sikre fremkommelighet til hjemmeboende brukere, eller hvordan ambulanser og nødetater skal sikres tilgang til helseinstitusjoner og omsorgsboliger ved stengte veier. Evakueringsplanen for helseinstitusjoner og omsorgsboliger regulerer evakuering fra bygg, men angir ikke hva som skal gjøres dersom veien til det angitte evakueringsstedet er stengt – Utskarpen bosenter er for eksempel angitt med Menighetshuset som evakueringssted uten at fremkommelighet er omtalt. Sektorplanen inneholder en oversikt over transportressurser, herunder om lag 80 leasingbiler og én minibuss, men omtaler ikke hva som skal gjøres dersom disse ikke kan nå brukere eller institusjoner som følge av stengte veier.

Sykehjem skal ifølge sektorplanen ha egne beredskapsplaner. Per revisjonstidspunktet har sykehjemmene ikke egne beredskapsplaner, men har benyttet sektorplanen for helse og mestring. Rana kommune opplyser at det pågår et arbeid med å utarbeide en felles beredskapsplan for alle sykehjemmene, koordinert med beredskapskoordinator og beredskapsnettverket. Et førsteutkast er ferdigstilt, men planene er ikke vedtatt. Det opplyses at bortfall av kritisk vei ikke har vært et fokusområde i dette arbeidet. Under forvaltningsrevisjonen utarbeidet kommunen en ROS-analyse som vurderer risikoen for at ansatte, nødetater eller forsyninger ikke kommer inn til kommunens fire sykehjem ved bortfall av kritisk vei. Analysen konkluderer med lavt risikonivå for samtlige sykehjem, begrunnet i flere alternative tilførselsveier. Kommunen opplyser at analysen vil bli inkludert i det pågående arbeidet med beredskapsplan for sykehjemmene.

5.3.4 Kompetanse, opplæring og øvelser

Kompetansebehov og system for opplæring

Kommunens overordnede beredskapsplan legger ansvaret for opplæring av de ansatte til linjeorganisasjonen. Overordnet planverk legger til grunn at sektorenes beredskapskoordinatorer månedlig gjennomfører trening i Rayvn, og som minimum har

[36] Stengingslenker er definerte veistrekninger i det nasjonale veidatasystemet som angir hvilke veilenker (veisegmenter) som skal stenges ved en gitt hendelse, og som danner grunnlag for omkjøringsruter. Kommunal veimyndighet plikter etter veidata- og trafikkinformasjonsforskriften § 14-1 å registrere slike lenker i Nasjonal veidatabank (NVDB).

grunn- og videregående kurs i programmet. Sektorenes beredskapsgrupper skal ha grunnkurs i Rayvn, og annethvert år gjennomføre trening i Rayvn.

I intervju pekes det på at teknisk sektor har forbedringspotensial når det gjelder opplæring. Det er ikke gjort en analyse av hvilken beredskapskompetanse teknisk sektor har behov for, og det følges ikke opp hvorvidt nyansatte setter seg inn i beredskapsplanverket. Det er heller ikke etablert system eller rutiner for opplæring av nyansatte i sektoren i henhold til de føringene om opplæring som følger av det overordnede beredskapsplanverket. Samtidig blir det i intervju vist til at opplæring i beredskap i sektoren er krevende, ettersom kompetansebehovet innad i sektoren er for differensiert til at et felles kurs vil være hensiktsmessig. Videre blir det pekt på at god kompetanse i daglige arbeidsoppgaver gir bedre forutsetninger for å håndtere en krise, og sentrale personer sektoren vurderer at denne kompetansen generelt er på et godt nivå, noe som også medvirker til at beredskapskompetansen også vurderes som god.

Opplæring og øvelser

Sektorberedskapsplan for tekniske tjenester fastslår at sektoren skal delta på alle øvelser som gjennomføres i regi av kommunens kriseledelse. Det er ikke utarbeidet en egen øvingsplan for sektoren tekniske tjenester. Seksjon samferdsel har heller ikke en egen øvingsplan, men deltar i øvelser i kommunal regi og i øvelser i regi av brann og redning der samferdsel er relevant.

Avdelingen brann og redning har en egen øvingsplan for 2026 med om lag 50 planlagte øvelser fordelt over hele året. Av øvelser særlig relevante for naturhendelser og bortfall av kritisk vei, er det planlagt øvelser med tema ekstremvær/skred, veitrafikkulykke, brann/ulykke i tunnel, trafikk og naturkatastrofe, samt samøvelse med MIP/industrivernet og sambandsøvelse. Øvingsplanen inneholder HMS-tema på hver øvelse og angir ansvarlig person.[37]

Som nevnt i kapittel 3.3.4 deltok kommunen på spilløvelsen «Øvelse Nordland 2024» i regi av Statsforvalteren i Nordland, med temaområdet «natur/vær».[38] Deltakerne inkluderte kommunaldirektørene, beredskapskoordinatorer, ordfører, kommunikasjonssjef og representanter fra Heimevernet, Røde Kors, Politiet, Sivilforsvaret og nabokommunene Nesna, Træna og Lurøy. Hensikten var å trene KKL, teste beredskapsplaner og identifisere svakheter ved ekstremværhendelser, med scenario tett knyttet til scenario 1 i helhetlig ROS.

5.3.5 Evaluering og forbedring

Sektorberedskapsplanen for tekniske tjenester fastslår at hendelser som har ført til at lokal beredskapsstab settes, skal evalueres av beredskapsstaben så snart hendelsen er avklart og situasjonen normalisert.[39] Evalueringsskjema er vedlagt beredskapsplanen, og evalueringsrapporten skal lagres i Rayvn. Planen beskriver ikke hvordan evalueringer skal følges opp med tiltak der det identifiseres å være behov for dette.

[37] Rana brann og redning. *Rana brann og redning 2026 øvingsplan*. Uten dato, oversendt 13.02.2026.
[38] Rana kommune. *Beredskapsøvelse: Øvelse Nordland 2024*. Melding. Registrert 23.01.2024.
[39] Rana kommune. *Sektorplan beredskap for tekniske tjenester 2024-2027 Rana kommune*. Vedtatt av kommunaldirektør tekniske tjenester 20.9.2024.

Som omtalt tidligere i rapporten, ble det utarbeidet en evalueringsrapport fra spilløvelsen «Øvelse Nordland 2024» i regi av Statsforvalteren, med tema ekstremvær. Rapporten inneholder punkter om hva som fungerte bra og mindre bra, og inkluderer oppfølgingstiltak relatert til revisjon av planverk, rutiner, opplæring og ressurser. Fem av ti oppfølgingstiltak er markert som utførte; de resterende fem er ikke gjennomført innen fristen 01.02.2024.

Revisjonen er videre forelagt evalueringer av to hendelser der værforhold førte til bortfall av EKOM. Evalueringene følger malen fra overordnet beredskapsplan og inneholder beskrivelse av hendelsesforløp og oppsummering av hva som fungerte bra og dårlig. Hendelsen 27.–29. desember 2025 er også relevant for bortfall av kritisk vei: Helgelandsbrua var stengt i perioder, og på det meste var 80 prosent av basestasjonene i kommunen ute av drift. Evalueringen identifiserte 34 forbedringstiltak, og tabellen med beskrivelse av tiltak inneholder oversikt over ansvarlige og tidsfrister. De fleste tiltakene har frist «Vår 2026».

Brann og redning har en fast rutine for gjennomføring av evalueringer, med tilhørende mal og støtteark. Støttearket legger opp til en strukturert evaluering i fire faser, med dialogregler og fem trinn for erfaringslæring. Evalueringen skal munne ut i konkrete læringspunkter kategorisert som «fortsette med», «slutte med» og «begynne med». Revisjonen er oversendt flere eksempler på utfylte evalueringer etter øvelser i brann og redning. Øvingsplanen til brann og redning inneholder også en planlagt evaluering av årets aktivitet i uke 52, 2026.

I intervju fremkommer det at avdeling drift infrastruktur har fast praksis for å evaluere gjennomføring av øvelser og håndtering av oppståtte hendelser, men at dette ikke følger en formalisert prosess. Evaluering skjer som del av det daglige arbeidet, og tiltak følges opp gjennom linjen. Det fremkommer videre at det ikke foreligger en fastsatt rutine for å omsette funn fra evalueringer til oppdatering av planverk. Saker som fremkommer gjennom hendelser, drift og evalueringer vurderes i forbindelse med den årlige revisjonen av planverket, som kvalitetssystemet varsler om. Det pekes på at det er noe personavhengig om og hvordan tilbakemeldinger fra operative nivåer formidles og innarbeides i planverket, og at nyanser av problemer kan forsvinne på veien oppover i systemet som følge av dette. Det opplyses videre at kapasitetsutfordringer i avdelingen til dels har påvirket oppfølgingen.

5.3.6 Samarbeid og samhandling

Kommunens samarbeid og samhandling med interne og eksterne beredskapsaktører er omtalt i kapittel 3. I det følgende omtales forhold som er spesifikt relevante for samarbeid og samhandling ved bortfall av kritisk vei.

Scenario 1 i helhetlig ROS forutsetter sektorovergripende håndtering og samhandling med en rekke eksterne aktører ved ekstremvær som isolerer en bygd. Samvirke er videre forankret i handlingsplanen i Plan for brann og redning, som inneholder konkrete tiltak for å styrke samarbeidet med interne og eksterne aktører, herunder tiltak for å videreutvikle samarbeidet med helsetjenestene og hjemmetjenestene, revidere samvirkeavtaler med Mo Industripark og nabobrannvesen, og etablere faste møtepunkter med kommunene. Tiltakene er planlagt gjennomført i første eller andre kvartal 2026.

Som omtalt i kapittel 3 og 5.3.4 hadde spilløvelsen «Øvelse Nordland 2024» ekstremvær som tema[40], og evaluering av øvelsen viste behov for å etablere flere avtaler om interkommunalt samarbeid knyttet til kritisk infrastruktur og naturhendelser.

Evalueringen av EKOM-hendelsene i desember 2025 avdekket samhandlingsutfordringer som også er relevante for scenario bortfall av kritisk vei. Helgelandsbrua var stengt i perioder under hendelsen, og bortfall av mobilnett og nødnett medførte at etablerte kommunikasjonskanaler mellom kommunens sektorer og mellom kommunen og eksterne aktører ikke fungerte. Blant de identifiserte forbedringstiltakene fra evalueringen er flere relevante for teknisk sektor og bortfall av kritisk vei, herunder revisjon av teknisk beredskapsplanverk med innarbeiding av mulighet for patruljering ved sambandsbrudd, etablering av kontaktpunkt (SPOC) for driftsenhetene utenfor arbeidstid, og gjennomføring av en fullskalaøvelse med scenario som omfatter både bortfall av EKOM og utilgjengelig vei.

I intervju fremkommer det at kommunen ved brokollaps etablerer fysiske sperringer for å forhindre at kjøretøy havner i elven, og deretter kontakter Statens vegvesen, som videreformidler til Forsvaret, som har lager med reservebroer. Kommunen disponerer ikke egne reservebroer. Det opplyses videre at kommunen har fått tildelt et direktenummer til veitrafikksentralen, slik at kontakt kan opprettes ved behov uten å benytte det ordinære publikumsnummeret.

5.4 Vurderinger

5.4.1 Roller og ansvar

Sektorberedskapsplanen for teknisk sektor angir overordnede fullmakter, prosess for eskalering, varslingsliste over relevante aktører og tiltakskort som fordeler oppgaver mellom avdelingene ved ulike hendelser. Det foreligger videre en varslingsplan for avdeling drift infrastruktur. Etter Deloittes vurdering er dette i samsvar med krav som følger av forskrift om kommunal beredskapsplikt § 4 knyttet til disse punktene. Deloitte merker seg også at likhetsprinsippet er innarbeidet i beredskapsarbeidet, ved at ansattes oppgaver i ordinær drift og i beredskapssituasjoner er sammenfallende, noe Deloitte mener fremstår hensiktsmessig.

Sektorberedskapsplanen for teknisk sektor beskriver samtidig ikke hvem som inngår i beredskapsstaben eller deres roller og ansvar. Deloitte mener dette ikke er i samsvar med kravene i forskrift om kommunal beredskapsplikt § 4 bokstav a om tydelig definering av roller og ansvar i beredskapssituasjoner innen sektoren, herunder hvem som inngår i beredskapsstaben og hvilket ansvar, detaljerte fullmakter og oppgaver disse har og skal ivareta. Deloitte vil understreke at dette er viktig å ha på plass, for å sikre en tydelig og ryddig organisert oppfølging av uønskede kritiske hendelser der slike skulle inntreffe.

Kommunens ansvar som kommunal veimyndighet for trafikkberedskap på eget veinett, jf. vegloven § 10 og veidata- og trafikkinformasjonsforskriften § 14-1, fremkommer ikke av sektorberedskapsplanen. Etter Deloittes vurdering bør kommunen sikre at det selvstendige ansvaret etter veglova § 10 er tydelig operasjonalisert i

[40] Rana kommune. *Beredskapsøvelse: Øvelse Nordland 2024.* Melding. Registrert 23.01.2024.

beredskapsplanverket, herunder at det fremgår hvem som ivaretar ansvaret i praksis og hvordan dette skal følges opp.

5.4.2 Risiko- og sårbarhetsanalyser knyttet til ødeleggelse av kritiske veier

Kommunen har vurdert risiko for ekstremvær og bortfall av kritisk vei gjennom både helhetlig ROS og ROS for brann og redning, og scenarioet er også omtalt i strategiske planer. Etter Deloittes vurdering er dette i samsvar med kravene til ROS-analyser som følger av sivilbeskyttelsesloven § 14 og forskrift om kommunal beredskapsplikt § 2.

Kommunen opplyser at den forholder seg til overordnet ROS og NVEs faresonekart i forbindelse med håndtering av hendelser som fører til at kommunale veier ikke er fremkommelige/kan benyttes som følge av ekstremvær og andre hendelser som fører til bortfall. Det foreligger utover disse opplysningene ingen dokumentasjon av at kommunen som kommunal veimyndighet har gjennomført risiko- og sårbarhetsanalyser som spesifikt danner grunnlag for trafikkberedskapsplaner og omkjøringsruter for kommunale veier, jf. veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav e. Etter Deloittes vurdering er dette ikke i samsvar med forskriftskravet. For å sikre at kravet innfris og at tilfredsstillende, helhetlig trafikkberedskap for hendelser som knytter seg til naturfare og værrelaterte farer er ivaretatt, mener Deloitte at Rana kommune må gjennomføre slike analyser og legge disse til grunn for trafikkberedskapsplaner for det kommunale veinettet.

Status for de foreslåtte tiltakene i helhetlig ROS knyttet til ekstremvær-scenarioet er ikke fullt ut avklart. Enkelte tiltak viser til et system som ikke lenger er i bruk, og statusoversikten viser tiltak som ikke er avsluttet. Etter Deloittes vurdering bør kommunen sikre en systematisk oppfølging av risikoreduserende tiltak identifisert gjennom ROS-arbeidet, eksempelvis gjennom etablering av rutiner for oppfølging med tydelig ansvarsplassering, krav til statusoppdatering og rapportering av fremdrift, jf. forskrift om kommunal beredskapsplikt § 3 om plan for oppfølging av samfunnssikkerhets- og beredskapsarbeidet.

5.4.3 Beredskapsplanverk

Teknisk sektor har utarbeidet med utgangspunkt i helhetlig ROS og relevante scenarier i denne som gjelder ekstremvær og hvordan dette kan påvirke kritiske veiinfrastruktur negativt, utarbeidet en sektorberedskapsplan i samsvar med kravene i forskrift om kommunal beredskapsplikt § 4. Deloitte vil samtidig peke på at beredskapsplanverket ikke omhandler bortfall av kritisk vei som et selvstendig scenario, og tiltakskortet for ekstremvær som isolerer en bygd som er utarbeidet, ikke inneholder konkrete opplysninger om hvordan en slik hendelse vil håndteres i praksis. Kommunen har heller ikke utarbeidet prosedyrer for trafikkberedskap, omkjøringsruter eller stengningslenker for kommunale veier, jf. veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav b til d.

Kommunen har bekreftet at det ikke er gjennomført en kategorisering av det kommunale veinettet eller utarbeidet trafikkberedskapsplaner i henhold til veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav b til d, f og g. Som omtalt i kapittel 5.4.2 foreligger det heller ikke risiko- og sårbarhetsanalyser som spesifikt danner grunnlag for slike planer. Etter Deloittes vurdering bør kommunen utarbeide

trafikkberedskapsplaner for aktuelle kommunale veistrekninger, herunder omkjøringsruter og stengningslenker, i samråd med øvrige veimyndigheter. Dette for å sikre god beredskap ved hendelser som fører til at kritiske veier må stenge, slik at trafikk i forbindelse med en hendelse kan fremføres på best og tryggest mulige måter for alle som ferdes på kommunens vegnett.

Deloitte registrerer at kommunen under forvaltningsrevisjonen har utarbeidet en ROS-analyse som vurderer risikoen ved bortfall av kritisk vei for drift og pasientsikkerhet ved hvert av de fire sykehjemmene i Rana, og vurderer det som positivt at kommunen har tatt dette initiativet. Analysen konkluderer med lavt risikonivå for samtlige sykehjem og vil ifølge kommunen inngå i det pågående arbeidet med egen beredskapsplan for sykehjemmene. Beredskapsplanen er imidlertid ikke ferdigstilt på revisjonstidspunktet, og Deloitte vil understreke viktigheten av at kommunen ferdigstiller denne og innarbeider vurderingene fra ROS-analysen, jf. forskrift om kommunal beredskapsplikt § 4. Deloitte vil videre peke på at sektorplanen for helse og mestring ikke omtaler hvordan hjemmetjenestene skal håndtere situasjoner der ansatte, nødetater eller forsyninger ikke når frem til hjemmeboende brukere grunnet bortfall av kritisk vei. Sektorplanen inneholder en oversikt over transportressurser, men vurderer ikke hva som skal gjøres dersom disse ikke kan nå brukere eller institusjoner som følge av stengte veier. Etter Deloittes vurdering bør kommunen sikre at beredskapsplanverket for helse og mestring også adresserer hjemmetjenestenes håndtering av slike situasjoner, jf. forskrift om kommunal beredskapsplikt § 4, og i samsvar med den overordnede risikovurderingen i RanaROS scenario 1 om isolering av bygd.

5.4.4 Opplæring og øvelser

Grunnleggende beredskapsopplæring i teknisk sektor bør formaliseres for å sikre systematikk og redusere sårbarhet ved personellutskiftninger, jf. forskrift om kommunal beredskapsplikt § 7. Det registrerer at likhetsprinsippet står sterkt i kommunens beredskapsarbeid og håndtering av hendelser som inntreffer, samt at kommunen over tid har bygget opp det den selv vurderer som god praktisk kompetanse og erfaring med beredskap på veg, grunnet bl.a. flere hendelser som har krevd involvering fra mange ansatte. Deloitte vil imidlertid understreke at formalisert og strukturert opplæring er nødvendig for å sikre at behovet for kompetanse på beredskap blir ivaretatt på en systematisk måte, slik at robusthet og kontinuitet i beredskapsarbeid på veg sikres over tid.

Deloitte registrerer at det nylig er gjennomført øvelse med tema ekstremvær, og at det er planlagt relevante øvelser innen samme tema for brann- og redningstjenesten. Deloitte registrerer også at det har blitt gjennomført øvelse (Øvelse Nordland 2024) der beredskap ved ødeleggelse av veiinfrastruktur inngikk, og der det ble øvd sammen med nabokommuner og beredskapsaktører, jf. krav i forskrift om kommunal beredskapsplikt § 7 og veidata- og trafikkinformasjonsforskriften § 14-2. Deloitte merker seg samtidig at det ikke foreligger en samlet øvingsplan for teknisk sektor som legger opp til systematiske beredskapsøvelser for relevant personell som omfatter ødeleggelse av kritiske veier. For å sikre at den planlagte beredskapen for håndtering av hendelser som fører til ødeleggelse av vei er godt kjent blant alle ansatte, samt fungerer i samsvar med intensjonene, mener Deloitte at det en plan som sikrer systematisk øvingsaktivitet på tvers av avdelingene i sektoren bør utarbeides.

5.4.5 Evaluering og forbedring

Kommunen har etablert rutiner for evaluering av øvelser og hendelser på flere nivåer, og Deloitte vurderer at disse ivaretar kravene i forskrift om kommunal beredskapsplikt § 8. Sektorberedskapsplanen inneholder evalueringsskjema, overordnet beredskapsplan har egen mal, og brann og redning har en fast rutine med tilhørende mal og støtteark. Undersøkelsen viser at evalueringer gjennomføres i praksis. Evalueringsrapportene fra brann og redning fremstår som ryddige og tydelige arbeidsverktøy, og det er etter Deloittes vurdering også positivt at det er planlagt en samlet evaluering av årets aktivitet ved utgangen av 2026. Evalueringen etter EKOM-hendelsen i desember 2025 følger malen i overordnet beredskapsplan og fremstår som hensiktsmessig utformet.

Samtidig er det Deloittes vurdering at oppfølgingen av funn i evaluering etter øvelser, kan forbedres. Gjennomgangen viser blant annet at identifiserte oppfølgingspunkt etter evaluering av Øvelse Nordland 2024, ikke er direkte koblet til identifiserte forbedringstiltak, og at halvparten av oppfølgingspunktene heller er ikke markert som utførte. Deloitte merker seg også opplysningene om at evaluering fremstår som en personavhengig og uformalisert prosess i enkelte avdelinger.

5.4.6 Samarbeid og samhandling

Rana kommune har etablert eksternt samarbeid relevant for håndtering av hendelser som fører til ødeleggelse av kritiske veier, og Deloitte vurderer det som positivt at samarbeidene er formalisert i avtaler, jf. forskrift om kommunal beredskapsplikt § 5. Samvirke med andre aktører etter samvirkeprinsippet, er integrert som element både i vurderingen av og øvingen på bortfall av kritisk vei ved naturhendelser.

Samtidig viser evalueringen av EKOM-hendelsene i desember 2025 at samhandlingen mellom sektorer og med eksterne aktører ble vesentlig svekket da etablerte kommunikasjonskanaler falt bort. Bortfall av kommunikasjon er en sannsynlig følgehendelse ved ekstremvær som også kan føre til bortfall av kritisk vei, jf. scenario 1 i helhetlig ROS. Etter Deloittes vurdering understreker dette viktigheten av at kommunen har samhandlingsrutiner som ikke er avhengige av ordinære kommunikasjonskanaler. Deloitte merker seg at kommunen har identifisert relevante forbedringstiltak, og vil understreke viktigheten av at disse tiltakene følges opp.

Kommunen opplyser at den samarbeider med andre offentlige etater på overordnet nivå om trafikkberedskap, men det foreligger ikke dokumentasjon som viser at kommunen har etablert formelt samarbeid spesifikt om trafikkberedskap, omkjøringsruter og stengningslenker for det kommunale veinettet, jf. veidata- og trafikkinformasjonsforskriften § 14-1 andre ledd bokstav c og § 14-2. Etter Deloittes vurdering bør kommunen formalisere samarbeidet med Statens vegvesen og fylkeskommunen om trafikkberedskap for det kommunale veinettet, og sikre at det dekker de beredskapsbehovene kommunen har.

6 Konklusjon og anbefalinger

Formålet med forvaltningsrevisjonen har vært å undersøke om Rana kommune har etablert tilstrekkelige systemer og rutiner for å sikre at kommunen er godt nok forberedt på å håndtere uønskede hendelser og krisesituasjoner, for å unngå at innbyggernes liv og helse settes i fare eller at vesentlige verdier går tapt.

Overordnet beredskap

Undersøkelsen viser at Rana kommune har etablert en overordnet beredskap som ivaretar de fleste sentrale kravene i regelverket, herunder krav om helhetlig risiko- og sårbarhetsanalyse forankret i kommunestyret, overordnet beredskapsplan med definerte roller og fullmakter, samarbeidsavtaler med eksterne aktører og et beredskapsnettverk for samhandling på tvers av sektorer. Kommunen gjennomfører også flere beredskapsøvelser hvert år.

Undersøkelsen identifiserte samtidig noen forbedringsområder i kommunens overordnede arbeid med samfunnssikkerhet og beredskap. Deloitte vil peke på at:

- Beredskapskoordinatorene sine roller og ansvar er ikke definert i overordnet beredskapsplan, og det fremstår uklart hva som er sentral beredskapskoordinators rolle ved håndtering av hendelser på sektornivå, herunder når og hvordan vedkommende skal involveres for å sikre at koordinators kompetanse og helhetsperspektiv bringes inn i sektorarbeidet.
- Ikke alle risikoreduserende tiltak som er identifisert gjennom ROS-analysen er fulgt opp og iverksatt.
- Sektorplan for oppvekst og kultur er ikke ferdigstilt, selv om arbeidet med denne hadde frist oktober 2024. At en hel sektor mangler et eget beredskapsplanverk, reduserer sektorens forutsetninger for å håndtere hendelser.
- En del beredskapsplaner er ikke oppdatert årlig i tråd med kommunens egne rutiner.
- Kommunen har ikke utarbeidet en samlet oversikt over hvilke enhets- og delplaner som foreligger på tvers av virksomhetene.
- Det er ulike oppfatninger av om kommunen har tilstrekkelig kapasitet i det forebyggende beredskapsarbeidet. Manglende oppdatering av planverk og oppfølging av tiltak i samsvar med frister kan indikere at kapasiteten ikke er tilstrekkelig.
- Kommunen har etablert et rammeverk for opplæring med kompetansekrav og øvelsesfrekvens for de ulike rollene i beredskapsorganisasjonen, men opplæringen er ikke dokumentert på en måte som gjør det mulig å ettergå om alle med roller i krisehåndteringen har fått opplæringen planen forutsetter. Kommunen har ikke gjennomført alle øvelsene i overordnet øvingsplan, og enkelte sektorer mangler øvingsplaner.
- Kommunen har etablert rutiner for evaluering av øvelser og hendelser, men oppfølgingen av identifiserte læringspunkter er ikke tilstrekkelig systematisk. Statusoversikten per april 2026 viser at i overkant av en tredjedel av tiltakene etter EKOM-hendelsene ikke er påbegynt, selv om fristene er passert.
- Beredskapsrådet har ikke vært operativt over en lengre periode, noe som ikke er i samsvar med DSB sin veileder til forskrift om kommunal beredskapsplikt.

- EKOM-hendelsene i desember 2025 avdekket svakheter i samhandlingen mellom sektorer, herunder manglende varsling og forsinket informasjon til befolkningen. Kommunal kriseledelse ble ikke satt, til tross for at flere av planverkets egne kriterier for dette fremstod som oppfylt.

Håndtering av cyberangrep

Undersøkelsen viser at kommunen har etablert et rammeverk for digital sikkerhet og beredskap gjennom overordnede styringsdokumenter, en formalisert sikkerhetsorganisasjon, implementering av ulike tekniske sikkerhetstiltak og samarbeid med eksterne kompetansemiljøer som KommuneCERT og Helse-CERT. IKT-avdelingen har høy teknisk kompetanse og har arbeidet systematisk med nettverkssegmentering og andre sikkerhetstiltak. Kommunen arbeider også systematisk med evaluering og forbedring.

Undersøkelsen viser samtidig noen områder med forbedringspotensial i arbeidet med beredskap knyttet til håndtering av cyberangrep. Deloitte vil peke på at:

- [redacted]
- Det foreligger ikke oppdatert systemspesifikk risikovurdering for det forretningskritiske systemet Profil omsorg, og det er ikke utarbeidet dedikerte tiltakskort for bortfall av systemet.
- Ansvarsfordelingen mellom IKT-avdelingen, sektorene og ekstern driftsleverandør er ikke tilstrekkelig tydelig kartlagt på alle områder (jf. NSM grunnprinsipp 1.3).
- Vesentlig kompetanse innen IKT-sikkerhet er konsentrert hos få personer, noe som gjør arbeidet personavhengig og medfører risiko for kommunens evne til å opprettholde et forsvarlig sikkerhetsnivå over tid.
- Det er ikke sikret at ansatte med beredskapsansvar for forretningskritiske systemer har tilstrekkelig innsikt i overordnede ROS-analyser og cyberangrepsscenarioer, noe som svekker grunnlaget for tilpassede beredskapsplaner og tiltakskort (jf. NSM grunnprinsipp 1.3). Det operative cyberangrepsplanverket er videre plassert på avdelingsnivå, noe som innebærer en risiko for at alvorlige digitale hendelser ikke i tilstrekkelig grad forankres og koordineres på overordnet ledelsesnivå, jf. NSM grunnprinsipp 1.1 og 4.1.

Ødeleggelse av kritiske veier

Undersøkelsen viser at kommunen har vurdert risiko for ekstremvær og bortfall av kritisk vei gjennom helhetlig ROS og ROS for brann og redning, og at scenarioet er prioritert som det første scenarioet i helhetlig ROS. Teknisk sektor har utarbeidet en beredskapsplan med tiltakskort for hvert av scenarioene i helhetlig ROS, og den inneholder videre varslingslister og eskaleringsrutiner. Teknisk sektor disponerer operative ressurser, herunder maskinpark, brøytekontrakter og nødnettskapasitet, og har inngått samarbeidsavtaler med relevante beredskapsaktører, noe som bidrar til å sette kommunen i stand til å håndtere en hendelse som medfører bortfall av kritisk vei.

Undersøkelsen viser samtidig noen områder med forbedringspotensial beredskapen knyttet til bortfall av kritisk vei. Deloitte vil peke på at:

- Kommunen har ikke kategorisert det kommunale veinettet eller utarbeidet trafikkberedskapsplaner med omkjøringsruter og stengningslenker, jf. veidata- og trafikkinformasjonsforskriften § 14-1.
- Det foreligger ikke risiko- og sårbarhetsanalyser som spesifikt danner grunnlag for trafikkberedskapsplaner og omkjøringsruter for kommunale veier.
- Det foreligger ikke formelt samarbeid med andre veimyndigheter spesifikt om trafikkberedskap, omkjøringsruter og stengningslenker for det kommunale veinettet.
- Det mangler øvingsplan og formalisert beredskapsopplæring for teknisk sektor. Evaluering av forbedringspunkter i avdeling drift infrastruktur skjer uten formalisert prosess, og oppfølging av funn fremstår personavhengig.
- Sektorberedskapsplanen for teknisk sektor definerer ikke hvem som inngår i beredskapsstaben eller deres roller og ansvar.
- Beredskapsplanverket adresserer ikke hvordan kommunen håndterer situasjoner der bortfall av kritisk vei hindrer fremkommelighet til beboere med behov for helsehjelp.

Anbefalinger

Basert på funn og vurderinger i undersøkelsen anbefaler Deloitte at Rana kommune iverksetter følgende tiltak:

1. Tydeliggjøre beredskapskoordinatorenes roller og mandat i håndteringen av hendelser i overordnet beredskapsplan.
2. Sørge for at kommunen har oppdaterte beredskapsplaner som dekker de mest sårbare risikoområdene.
3. Utarbeide en oversikt over alle beredskapsplanene i kommunen, og vurdere å legge denne inn i overordnet beredskapsplan.
4. Reetablere beredskapsrådet som arena for samordning med eksterne aktører.
5. Sørge for at KKL blir etablert når kriteriene for dette er oppfylt.
6. Sørge for at identifiserte forbedringstiltak blir fulgt opp i samsvar med satte frister.
7. Sørge for at det foreligger oppdaterte risikovurderinger for alle forretningskritiske systemer.
8. Tydeliggjøre roller og ansvar mellom systemansvarlig, IKT-avdelingen og ekstern driftsleverandør.
9. Utarbeide risikovurderinger og kategorisere det kommunale veinettet.
10. Utarbeide trafikkberedskapsplaner for det kommunale veinettet i samråd med øvrige veimyndigheter.
11. Sikre at teknisk sektor sin beredskapsplan definerer krisestabens sammensetning, roller og ansvar.
12. Vurdere å adressere bortfall av kritisk vei i beredskapsplanverket, herunder hvordan fremkommelighet til beboere med behov for helsehjelp skal sikres.

Vedlegg 1: IKT-prosedyrer, -rutiner og -retningslinjer

Tabell 6: Overordnede retningslinjer for IKT-sikkerhet

Retningslinjer	Beskrivelse
Overordnet retningslinje for informasjonssikkerhet	Overordnet styringsdokument for informasjonssikkerhetsarbeidet. Fastslår mål og rammer basert på prinsippene konfidensialitet, integritet og tilgjengelighet, og krav om styringssystem etter ISO 27001.
Overordnet policy / retningslinje for autentiseringsinformasjon (passordpolicy)	Definerer krav til passordkvalitet for alle brukere, herunder krav om minimum 14 tegn og særskilte krav for privilegerte kontoer og servicekontoer.
Overordnet retningslinje / Policy for bruk av kunstig intelligens	Regulerer bruk av KI-tjenester på vegne av kommunen. Krever at KI benyttes til virksomhetsrelaterte formål, at konfidensiell informasjon ikke mates inn, og at risikovurdering gjennomføres før bruk.
Overordnet retningslinje / Policy for bruk og sikring av brukerutstyr	Definerer sikkerhetskrav for datamaskiner, nettbrett og mobiltelefoner, herunder krav om sikker konfigurasjon, antimalware, kryptering av bærbare enheter og begrensning av brukerrettigheter.
Overordnet retningslinje / Policy for fjernarbeid	Regulerer sikkerhetstiltak ved arbeid utenfor kommunens lokaler, herunder krav om bruk av kommunalt utstyr for konfidensiell informasjon og unngåelse av usikrede trådløse nettverk.
Overordnet retningslinje / Policy for kryptografi	Definerer krav til kryptografiske kontroller for å sikre konfidensialitet, integritet og autentisitet, herunder kryptering ved lagring og overføring, BitLocker for endepunkter og AES 256-bit for flyttbare medier.
Overordnet retningslinje / Policy for nettverkssikkerhet	Regulerer sikkerhetstiltak på nettverksnivå, herunder krav om dokumentasjon av nettverkskomponenter, kryptering av trafikk, oppdatering av firmware, logging og overvåking, nettverkssegmentering og filtrering av skadelige nettsteder.
Overordnet retningslinje / Policy for overføring av personopplysninger	Definerer rammer for overføring av personopplysninger til tredjeparter og internasjonale organisasjoner i samsvar med personvernlovgivningen.
Overordnet retningslinje / Policy for å ivareta de registrertes rettigheter	Definerer rammer for hvordan kommunen skal respektere og ivareta de registrertes rettigheter i samsvar med personvernregelverket.
Overordnet retningslinje for tilgangsstyring	Definerer prinsipper for tilgangsstyring til nettverk, IT-utstyr og informasjonssystemer, herunder rollebasert tilgangskontroll, minste-rettighets-prinsippet, jevnlig gjennomgang av tilganger, multifaktorautentisering for privilegerte kontoer og logging av tilgang.
Overordnet retningslinje for logging	Definerer krav til logging og sporbarhet i produksjonssystemer, herunder krav om tidssynkronisering, sikring mot endringer, lagringstid på minimum 13 måneder og innsending til SIEM-løsning.

Overordnet retningslinje for sikkerhetskopiering og gjenoppretting	Regulerer sikkerhetskopiering og gjenoppretting av informasjon og personopplysninger, herunder krav om kryptering av sikkerhetskopier, testing av gjenoppretting minimum årlig og dokumentasjon av RTO og RPO.
Overordnet retningslinje for kontinuerlig forbedring	Definerer rammer for kontinuerlig forbedring av styringssystemet for informasjonssikkerhet, herunder krav om evaluering av ytelse, identifikasjon og prioritering av forbedringsområder og tilstrekkelig opplæring og ressurser.

Tabell 7: Rutiner, prosedyrer og andre dokumenter knyttet til IKT-sikkerhet

Rutiner, prosedyrer, sjekklister, mv.	**Beskrivelse av innhold**
Sikkerhetsinstruks Rana kommune	Fastsetter plikter og regler for ansatte, folkevalgte og leverandører knyttet til informasjonstilgang, IT-bruk, passord, fysisk sikkerhet, varsling og avvikshåndtering.
Prosedyre for ledelsens gjennomgang - informasjonssikkerhet og personvern	Beskriver gjennomføring av årlig ledelsesgjennomgang, herunder deltakere, innhold, krav til vedtak og referatføring.
Inngåelse og registrering av en Databehandleravtale	Beskriver krav og prosess for inngåelse av databehandleravtaler, herunder bruk av DFØ-malen, risikovurdering og arkivering i Elements.
Prosedyre for sikkerhetskonfigurasjon i Microsoft 365	Beskriver mål og gjennomføring for å oppnå minimum 75 % Secure/Compliance Score i Microsoft 365, herunder roller og forbedringstiltak i Defender XDR og Purview.
Prosedyre for overvåking, måling, analyse og evaluering	Beskriver etablering av ISMS-dashboard med KPIer for kompetanse, modenhet, hendelser, risiko, samsvar og teknisk status, samt ansvar for måling og forbedring.
Rutine for løsepengetrussel - ransomware	Operativ prosedyre ved ransomware-angrep, herunder varsling, isolering, dokumentasjon, ekstern varsling, gjenoppretting og etterkontroll.
Sjekkliste for ansatte ved mistanke om ransomware	Enkel handleliste for ansatte ved mistanke om ransomware, herunder tegn på angrep, umiddelbare tiltak og varslingspunkter.
Prosedyre for håndtering av digitale bevis	Beskriver innsamling, sikring, lagring og overlevering av digitale bevis, herunder krav til integritetssikring og kjede av forvaring.
Krav om innsyn	Rutine for håndtering av innsynsbegjæringer etter GDPR artikkel 15, herunder unntak, begrunnelser ved avslag og informasjon til den registrerte.
Protokoll over behandlingsaktiviteter	Beskriver hvordan behandlingsprotokoll føres i Sureway, herunder roller, formål, rettslig grunnlag, kategorier, mottakere, lagringstid og databehandlere.
Rutine for Personvern-konsekvensvurdering (DPIA) og forhåndsdrøftelse	Beskriver formål, omfang og ansvar for DPIA, herunder når DPIA kreves, prosess-steg og kriterier for forhåndsdrøftelse med Datatilsynet.
Rutine - forhåndsdrøftelse Datatilsynet	Beskriver når og hvordan forhåndsdrøftelse med Datatilsynet skal gjennomføres, herunder krav til innhold og sikker oversendelse.

Avvikshåndtering og brudd på personopplysnings-sikkerheten	Beskriver definisjoner, ansvar og behandling av avvik, herunder varsling, strakstiltak, meldeplikt til Datatilsynet og oppfølging.
Prosedyre for å vurdere og å melde brudd/avvik på personopplysnings-sikkerheten til Datatilsynet	Beskriver vurdering av meldeplikt, frister, prosess i Altinn og dokumentasjonskrav ved melding av brudd på personopplysningssikkerheten til Datatilsynet.
Dokumentmal for intern forberedelse for sending av avvik til Datatilsynet	Utfyllingsmal som forbereder melding til Datatilsynet via Altinn, herunder årsak, omfang, berørte, konsekvenser og tiltak.

Vedlegg 2: Høringsuttalelse

Rana kommune

Mo i Rana, 08.05.2026

DELOITTE AS AVD BERGEN
Postboks 6013
5892 BERGEN

Saksnummer og dokumentnummer	Avdeling/saksbehandler	Deres referansenummer
2025/21457-3	STAB/STØTTE/HJO	

Høringsuttalelse- rapport forvaltningsrevisjon av samfunnssikkerhet og beredskap.

Kommunedirektøren har mottatt rapportutkast til forvaltningsrevisjon av samfunnssikkerhet og beredskap 4. mai 2026. Frist for å gi høringsuttalelse er 8. mai 2026.

Beredskapsoppgavene har økt som følge av endret trusselbilde. Som kommune må vi være forberedt på flere uønska hendelser og økte krav til sikkerhet- og beredskap.

Rana kommune jobber systematisk og helhetlig med samfunnssikkerhet og beredskap. Dette er et kontinuerlig arbeid som løpende må tilpasses endringer i trusselbildet. Ressurser og tiltak prioriteres basert på risiko og evaluering etter øvelse og hendelser.

Arbeidet med beredskap og samfunnssikkerhet krever kontinuerlig fokus. Å bli vurdert utenfra er en viktig del av vårt forbedrings- og utviklingsarbeid.

Statsforvalteren er tilsynsmyndighet og fører jevnlig tilsyn med kommunen med hjemmel i sivilbeskyttelsesloven § 29 og beredskapspliktforskriften § 10. Siste tilsyn ble gjennomført i 2023 uten avvik innen kommunal beredskapsplikt.

I mars 2026 har Statsforvalteren i Nordland vurdert området samfunnssikkerhet og beredskap som grønt i kommunebilde for Rana. «Kommunebilde» er et digitalt verktøy og en tilstandsrapport som Statsforvalteren i Nordland utarbeider for hver enkelt kommune. Her vurderes Rana å ha et solid system for ledelse og styring med beredskap integrert i strukturen. Både overordnet og sektorvise ROS-analyser vurderes å være av høy kvalitet. I tillegg har kommunen gode og oppdaterte beredskapsplaner i flere sektorer. Det trekkes

Rana kommune

også frem at Rana kommune har en kompetent og erfaren kriseledelse som kjenner godt til roller og ansvar, og har ved flere anledninger dokumentert god krisehåndtering.

Vi oppfatter at forvaltningsrevisjonsrapporten som nå er lagt frem i hovedtrekk samsvarer med statsforvalterens konklusjon om at Rana kommune har en beredskapsorganisasjon og et planverk som ivaretar sentrale krav i regelverket. Samtidig opplever vi at rapporten er på et mer detaljert nivå enn det vi hadde forventet av en forvaltningsrevisjon.

Rana kommune er en lærende organisasjon, opptatt av forbedring og utvikling. Undersøkelsen har identifisert noen forbedringsområder som vil bli fulgt opp slik av administrasjonen:

Plan for oppfølging :

Tiltak	Oppfølging	Innen
1. Tydeliggjøre beredskaps-koordinatorenes roller og mandat i håndteringen av hendelser i overordnet beredskapsplan.	Rollebeskrivelse i kvalitetsportal. Oppdatere overordnet planverk ved neste revisjonsrunde.	01.08.26
2. Sørge for at kommunen har oppdaterte beredskapsplaner som dekker de mest sårbare risiko områdene.	Ferdigstille beredskapsplan for sykehjemmene. Oppdatere beredskapsplanverk etter at helhetlig ROS er gjennomført.	30.8.26 Vår 2027
3. Utarbeide en oversikt over alle beredskapsplanene i kommunen, og vurdere å legge denne inn i overordnet beredskapsplan.	Legge alle planer inn på kommunens oversiktsside etablert for beredskapsplaner i kvalitetsportal.	30.8.26
4. Reetablere beredskapsrådet som arena for samordning med eksterne aktører.	Iverksette tidligere vedtak. Kalle inn til møte for reetablering.	30.08.26
5. Sørge for at KKL blir etablert når kriteriene for dette er oppfylt.	Vurdere situasjon og følge opp iht. planverk.	Løpende
6. Sørge for at identifiserte forbedringstiltak blir fulgt opp i samsvar med satte frister.	Følge opp oppgaver i EQS og sikre at de gjennomføres og avsluttes iht. etablerte rutiner. Gjennomføre opplæring i bruk av kvalitetssystemet.	Løpende Høst 2026

Rana kommune

7. Sørge for at det foreligger oppdaterte risikovurderinger for alle forretningskritiske systemer.	Gjennomføre DPIA og ROS knyttet til GDPR på Visma Profil. Gjennomføre ROS på nytt EPJ-system. Oppdatere risikovurderinger på øvrige forretningskritiske systemer.	30.9.26 Vår 2027
8. Tydeliggjøre roller og ansvar mellom systemansvarlig, IKT-avdelingen og ekstern driftsleverandør.	Kvalitetssikre etablerte rutiner.	01.07.26
9. Utarbeide risikovurderinger og kategorisere det kommunale veinettet.	Utarbeide risikovurdering og kategorisering av det kommunale veinettet.	Q2 2027
10. Utarbeide trafikkberedskapsplaner for det kommunale veinettet i samråd med øvrige veimyndigheter.	Innarbeides i beredskapsplan for teknisk sektor i revisjon 2026. Arbeid mot øvrige veimyndigheter ferdig i løpet av 1. halvår 2027	Q3 2026 Q2 2027
11. Sikre at teknisk sektor sin beredskaps-plan definerer krisestabens sammen-setning, roller og ansvar.	Innarbeides i revidert beredskapsplan	Q3 2026
12. Vurdere å adressere bortfall av kritisk vei i beredskapsplanverket, herunder hvordan fremkommelighet til beboere med behov for helsehjelp skal sikres.	ROS-bortfall av vei til sykehjem er gjennomført ROS-fremkommelighet til beboere med behov for helsehjelp	OK 30.9.26

Med vennlig hilsen

Hege Kristin Johansen Nygård
Kommunaldirektør stab

Brevet er elektronisk signert og har derfor ikke håndskrevne signaturer.

Vedlegg 3: Revisjonskriterier

Lov om kommunal beredskapsplikt, sivile vernetiltak og Sivilforsvaret (sivilbeskyttelsesloven)

Sivilbeskyttelsesloven §§ 14 og 15 fastsetter den kommunale beredskapsplikten. Kommunen plikter å kartlegge hvilke uønskede hendelser som kan inntreffe, vurdere sannsynligheten for at disse hendelsene skjer og hvordan de kan påvirke kommunen. Resultatet skal sammenstilles i en helhetlig risiko- og sårbarhetsanalyse som skal legges til grunn for kommunens arbeid med samfunnssikkerhet og beredskap. Analysen skal oppdateres i takt med revisjon av kommunedelplaner og ved endringer i risiko- og sårbarhetsbildet.

Med utgangspunkt i risiko- og sårbarhetsanalysen skal kommunen utarbeide en beredskapsplan med oversikt over tiltak for å håndtere uønskede hendelser. Beredskapsplanen skal som et minimum inneholde plan for kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media. Planen skal være oppdatert, revideres minimum én gang i året, og jevnlig øves.

Beredskapsplanen skal øves minst hvert annet år, og scenarioene bør hentes fra den helhetlige risiko- og sårbarhetsanalysen. Kommunen skal ha et system for opplæring som sikrer at alle med roller i krisehåndteringen har tilstrekkelige kvalifikasjoner. Etter øvelser og uønskede hendelser skal kommunen evaluere krisehåndteringen, og gjøre nødvendige endringer i analysen eller beredskapsplanene.

Forskrift om kommunal beredskapsplikt konkretiserer beredskapsplikten i sivilbeskyttelsesloven

Forskriften skal sikre at kommunen tar vare på sikkerheten til befolkningen gjennom systematisk og helhetlig samfunnssikkerhetsarbeid på tvers av sektorer, med sikte på å redusere risiko for tap av liv eller skade på helse, miljø og materielle verdier. Plikten omfatter kommunen som myndighet, som virksomhet og som pådriver overfor andre aktører.

Forskriften § 2 stiller minimumskrav til innholdet i den helhetlige risiko- og sårbarhetsanalysen. Analysen skal forankres i kommunestyret og omfatte eksisterende og fremtidige risiko- og sårbarhetsfaktorer, risiko utenfor kommunens geografiske område som kan ha betydning for kommunen, hvordan ulike faktorer kan påvirke hverandre, særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur, kommunens evne til å opprettholde og gjenoppta virksomheten ved uønskede hendelser, samt behov for befolkningsvarsling og evakuering.

På bakgrunn av analysen skal kommunen utarbeide langsiktige mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhetsarbeidet, jf. forskriften § 3. Kommunen skal også vurdere forhold som bør integreres i planer og prosesser etter plan- og bygningsloven.

Forskriften § 4 stiller krav til beredskapsplanen. Planen skal som et minimum inneholde:

a. *Plan for kommunens kriseledelse med opplysninger om hvem som utgjør kriseledelsen, deres ansvar, roller og fullmakter, og hvem som har fullmakt til å kalle inn kriseledelsen.*

b. Varslingsliste over aktører som har en rolle i krisehåndteringen. Kommunen skal informere alle på listen om deres rolle.

c. *Ressursoversikt med opplysninger om hvilke ressurser kommunen selv råder over og hva som er tilgjengelig hos andre aktører. Kommunen bør inngå avtaler om bistand under kriser.*

d. Evakueringsplaner og plan for befolkningsvarsling basert på den helhetlige risiko- og sårbarhetsanalysen.

e. *Plan for krisekommunikasjon med befolkningen, media og egne ansatte.*

f. Beredskapsplanen skal til enhver tid være oppdatert og som et minimum revideres årlig, jf. forskriften § 6. Av planen skal det fremgå hvem som har ansvar for oppdatering og når planen sist ble oppdatert.

Etter forskriften §§ 7 og 8 skal beredskapsplanen øves minst hvert annet år, og scenarioene bør hentes fra den helhetlige risiko- og sårbarhetsanalysen. Kommunen skal ha et system for opplæring som sikrer at alle med roller i krisehåndteringen har tilstrekkelige kvalifikasjoner. Etter øvelser og uønskede hendelser skal kommunen evaluere krisehåndteringen og gjøre nødvendige endringer i analysen eller beredskapsplanene.

Veileder til forskrift om kommunal beredskapsplikt (DSB, 2021) utdyper og konkretiserer kravene i sivilbeskyttelsesloven og forskriften. Veilederen presiserer at kommunal beredskapsplikt omfatter kommunen i tre roller: som myndighet innenfor sitt geografiske område, som virksomhet, og som pådriver overfor andre aktører.

a. *Et sentralt prinsipp er at samfunnssikkerhetsarbeidet skal være helhetlig og systematisk. Helhetlig innebærer at arbeidet skal omfatte alle faser i samfunnssikkerhetskjeden: oversikt og kunnskap, forebygging, beredskap, krisehåndtering og normalisering. Systematisk innebærer at kommunen skal ha etablerte rutiner for kontinuerlig forbedring av beredskapsarbeidet.*

b. *Veilederen legger til grunn at kravene i lov og forskrift skal tilpasses de konkrete risiko- og sårbarhetsutfordringene kommunen står overfor. Kommunen må utlede spesifikke krav basert på egen risiko- og sårbarhetsanalyse. En kommune med høy risiko for digitale angrep må for eksempel utarbeide beredskapsplaner og øvingsprogram tilpasset denne risikoen, selv om regelverket ikke eksplisitt nevner digitale hendelser.*

c. *Overordnet beredskapsplan er et av de viktigste virkemidlene i kommunens oppfølging av beredskapsplikten. Planen skal hjelpe kommunen å lede krisehåndteringen ved uønskede hendelser, og bør ha en generisk tilnærming slik at den er egnet til å håndtere ulike typer hendelser. I tillegg til minimumskravene kan planen inneholde særskilte prosedyrer og beredskapstiltak basert på funn i den helhetlige ROS-analysen.*

d. *Overordnet beredskapsplan skal samordne og integrere andre beredskapsplaner i kommunen, og være samordnet med relevante offentlige og private krise- og beredskapsplaner. Dette omfatter blant annet beredskapsplaner hos politi, Statens veivesen, helseforetak, energi- og nettselskap, risikovirksomheter og frivillige organisasjoner.*

e. *Plan for krisekommunikasjon er verktøyet kriseledelsen har for kommunikasjon med befolkningen, media og egne ansatte ved uønskede hendelser. Planen bør beskrive fordeling av roller og ansvar, og inneholde rutiner for samarbeid med andre samfunnssikkerhetsaktører slik at krisekommunikasjonen fremstår samordnet.*

Veilederen gir også veiledning om øving, opplæring og evaluering. Gjennom øvelser kan kommunen teste og videreutvikle beredskapsplanene, gi opplæring til de som inngår i kriseorganisasjonen, og avdekke sterke og svake sider i samfunnssikkerhetsarbeidet. Viktige øvingsmomenter er avklaring av roller og ansvar, etablering av situasjonsforståelse, fordeling av ressurser og krisekommunikasjon. Evalueringer bør planlegges samtidig med øvelsen, og de som har øvd bør samles rett i etterkant for å innhente førsteinntrykk.

Stortingsmelding 5 (2020-2021): Nasjonale prinsipper for arbeid med samfunnssikkerhet og beredskap

Det nasjonale samfunnssikkerhets- og beredskapsarbeidet er bygd på fire prinsipper: ansvar, nærhet, likhet og samvirke. Prinsippene er omtalt i Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden:

- **Ansvarsprinsippet**: Den som til vanlig har ansvaret for et område, har også ansvaret for nødvendige beredskapsforberedelser og tjenesten ved kriser. Dette omfatter planlegging av hvordan funksjoner skal kunne opprettholdes ved ekstraordinære hendelser.

- **Nærhetsprinsippet**: Kriser skal organisatorisk håndteres på lavest mulig nivå. Den som er nærmest krisen har vanligvis de beste forutsetningene for å forstå og håndtere situasjonen. Prinsippet gjelder ikke ved sikkerhetspolitiske kriser.

- **Likhetsprinsippet**: Organisasjonen som blir brukt under kriser bør være mest mulig lik den ordinære organisasjonen. Ansvarsforholdene internt og mellom virksomheter skal ikke endres ved krisehåndtering.

- **Samvirkeprinsippet**: Alle aktører har et selvstendig ansvar for å sikre best mulig samarbeid med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering.

NSMs grunnprinsipper for IKT-sikkerhet

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene er relevante for alle typer virksomheter, og ved å følge anbefalingene vil virksomheter få et godt fundament for sikkerheten i IKT-systemene. Grunnprinsippene er utarbeidet i samarbeid med

virksomheter som forvalter kritiske samfunnsfunksjoner og kritisk infrastruktur, og representerer beste praksis og anerkjente standarder for digital sikkerhet.

Rana kommune har ansvar for samfunnskritiske tjenester, som helsetjenester til innbyggerne, og tilhørende IKT-systemer. Uavhengig av om kommunen formelt er omfattet av digitalsikkerhetsloven, gir NSMs grunnprinsipper uttrykk for beste praksis og anerkjente standarder for digital sikkerhet som er relevante for kommunens arbeid med digital beredskap.

NSMs grunnprinsipper er fordelt på fire kategorier: 1) Identifisere og kartlegge, 2) Beskytte og opprettholde, 3) Oppdage, og 4) Håndtere og gjenopprette. Hvert grunnprinsipp inneholder tiltak som beskriver hva en virksomhet bør gjøre for å sikre informasjonssystemer og verdier. Grunnprinsippene fokuserer på teknologiske og organisatoriske tiltak, og kan danne en basis for bransjenormer og utdype IKT-anbefalinger i sektorregelverk. I denne revisjonen er grunnprinsippene brukt som revisjonskriterium for å vurdere kommunens arbeid med digital beredskap, og for å konkretisere hva som ligger i kravet om forsvarlig sikkerhet.

Styringsstrukturer og prosesser for sikkerhetsstyring (NSM grunnprinsipp 1.1)

Kommunen bør etablere og vedlikeholde strukturer og prosesser for sikkerhetsstyring som omfatter digital sikkerhet. Dette bør være dokumentert og inngå som en del av den overordnede styringen av kommunen. Roller og ansvar for digital sikkerhet bør defineres, utpekes og dokumenteres. Kommunen bør sikre at sikkerhetsstyringen omfatter alle nettverks- og informasjonssystemer som ligger til grunn for leveransen av tjenestene.

Sikkerhetsstyringen bør baseres på anerkjente standarder og bidra til å forebygge, avdekke og håndtere hendelser, korrigere og gjenopprette sikkerheten i nettverks- og informasjonssystemer ved hendelser, og kontinuerlig styre og følge opp at disse formålene blir oppnådd. Prosesser for sikkerhets- og risikostyring må tilpasses virksomheten.

Toppledelsen har fokus på organisatorisk risiko og bør ta eierskap til og involvere seg i sikkerhetsarbeidet i egen virksomhet. De ulike kategoriene og prinsippene i NSMs grunnprinsipper for IKT-sikkerhet kan brukes som styringsparameter i dette arbeidet. Sikkerhetsstyringen bør gjennomgås minst årlig med sikte på å bedre sikkerhetsarbeidet i kommunen.

Risikovurdering og risikostyring (NSM grunnprinsipp 1.1)

Kommunen bør gjennomføre risikovurderinger av nettverks- og informasjonssystemer som blir brukt for å levere tjenestene. Risikovurderingen bør være av et slikt omfang at kommunen kan identifisere organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak. Ved endringer i virksomheten som kan påvirke sikkerheten, bør kommunen vurdere hvilken risiko endringene medfører. Risikovurderinger bør utarbeides, vedlikeholdes og dokumenteres.

Risikovurderingen bør minst beskrive følgende:

a) Nettverks- og informasjonssystemene til virksomheten og hvilken betydning disse har for leveransen av den samfunnsviktige tjenesten

b) Hvilke hendelser nettverks- og informasjonssystemene til kommunen kan bli utsatt for

c) Hvilke sårbarheter som er knyttet til nettverks- og informasjonssystemene til virksomheten

d) Konsekvensen av hendelser

e) I hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal

Basert på risikovurderingen bør kommunen ha en plan for å håndtere risiko. Kommunen bør sette i verk egnede og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet sørger for et sikkerhetsnivå som er tilpasset risikoen. Sikkerhetstiltakene bør som et minimum ha som formål å bidra til sikker plattform, sikker drift og vedlikehold, og sikker hendelseshåndtering og gjenoppretting.

Organisatoriske sikkerhetstiltak (NSM grunnprinsipp 2.1-2.10)

Kommunen bør utarbeide skriftlige instrukser, rutiner og prosedyrer for digital sikkerhet, tilpasset størrelsen, kompleksiteten og risikobildet til virksomheten. Kommunen bør ha oppdaterte tiltaksplaner som kan settes i verk dersom risikoen endrer seg eller det oppstår en hendelse. Styringsdokumentene og tiltaksplanene bør gjøres kjent for personell som utfører oppgaver for eller på veine av kommunen og som kan få tilgang til nettverks- og informasjonssystemene.

Kommunen bør sette i verk teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved nettverks- og informasjonssystemene.

Følgende kategorier av teknologiske sikkerhetstiltak bør minst implementeres:

a) Sterk autentisering for tilgang til nettverks- og informasjonssystemer

b) Styring av og kontroll med tilganger til nettverks- og informasjonssystemene til kommunen

c) Tiltak for segmentering av nettverk og tjenester basert på prinsippet om minste privilegium

d) Tiltak som skal sikre at nettverks- og informasjonssystemer kan håndtere ulike typer avbrudd og gjenopprettes innen rimelig tid

e) Tiltak som skal sikre at nettverks- og informasjonssystem har tilstrekkeleg kapasitet til å tole overbelastning og utstyrsfeil

f) Tiltak som skal sikre at nettverks- og informasjonssystem vert vidareutvikla kontinuerleg, medrekna at oppdateringar vert kvalitetssikra, installerte og testa fortløpande

g) Sikkerheitsovervaking av nettverks- og informasjonssystem for å avdekkje hendingar

Kommunen bør setje i verk fysiske sikkerheitstiltak for å oppretthalde forsvarleg sikkerheit i nettverks- og informasjonssystem. Følgjande kategoriar av fysiske sikkerheitstiltak bør minst implementerast:

a) Tiltak for å hindre at uvedkommende får tilgang til lokasjoner og fysisk og teknisk infrastruktur som nettverks- og informasjonssystemer bruker eller er avhengige av

b) Tiltak for å identifisere og verne bygninger, rom og tilstøtende område som har betydning for sikkerhetsnivået

c) Tiltak for å ta vare på eksterne avhengigheter, medregnet datakommunikasjon og strømtilførsel

d) Tiltak for å avdekke hendelser med negativ virkning på sikkerheten

Sikkerhetstiltak for personell (NSM grunnprinsipp 1.3 og 2.6)

Kommunen bør sette i verk nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til nettverks- og informasjonssystemene. Dette bør sikres gjennom å:

a) Tildele tilgang til lokaler og tilganger til nettverks- og informasjonssystemer basert på roller, oppgaver, ansvar og tjenestlig behov, samt følge opp at personell ikke har flere tilganger enn nødvendig

b) Sikre at ansatte, leverandører og oppdragstakere er gjort kjent med relevante sikkerhetstiltak, har tilstrekkelig kompetanse innenfor sikkerhet og får nødvendig opplæring ved behov

Hendelseshåndtering og beredskap (NSM grunnprinsipp 4.1-4.4)

Kommunen bør ha en beredskapsplan for håndtering av hendelser og varsling om hendelser som virker vesentlig inn på tjenesteleveransen. Kommunen bør vurdere relevante beredskapstiltak og skjerping i eksisterende sikkerhetstiltak som raskt kan settes i verk ved behov.

Dersom kommunen er utsatt for en hendelse, bør karakteren og omfanget av hendelsen identifiseres, og kommunen bør sette i verk nødvendige mottiltak og tiltak for å gjenopprette den sikre tilstanden i nettverks- og informasjonssystemer. Kommunen bør utarbeide, vedlikeholde og dokumentere beredskapsplaner og gjennomføre øvelser for å teste planverket og utvikle kompetansen til å håndtere hendelser. Kommunen bør lære av hendelser og forbedre sikkerhetstiltak, hendelsesprosesser og opplæring av personell.

Kommunen bør uten ugrunnet opphold varsle om hendelser som virker vesentlig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er vesentlig, bør det blant annet legges vekt på antall brukere som blir påvirket, varigheten til hendelsen og størrelsen på det geografiske området som blir rammet.

Kommunen har en oppfølgingsplikt overfor leverandører og andre som utfører arbeid som kan påvirke sikkerheten i nettverks- og informasjonssystemene. Kommunen bør påse at slikt arbeid blir utført på en måte som gjør at kravene til forsvarlig sikkerhet blir overholdt. Kommunen bør gjennom avtale eller på annen egnet måte gjøre sikkerhetstiltakene gjeldende overfor leverandører, i den grad det er nødvendig for å opprettholde et forsvarlig sikkerhetsnivå. Oppfølgingsplikten gjelder uavhengig av om drift og vedlikehold av tjenesten er satt bort helt eller delvis til andre.

Vedlegg 4: Sentrale dokumenter og litteratur

Lov og forskrift

- Kommunal- og distriktsdepartementet: Lov om kommuner og fylkeskommuner (kommuneloven). LOV-2018-06-22-83
- Justis- og beredskapsdepartementet: Forskrift om kommunal beredskapsplikt. FOR-2011-08-22-894
- Justis- og beredskapsdepartementet: Lov om sivil beskyttelse og beredskap (sivilbeskyttelsesloven). LOV-2010-06-25-45

Forarbeider, rundskriv, veiledere mv.

- Direktoratet for samfunnssikkerhet og beredskap. *Veileder til forskrift om kommunal beredskapsplikt*. 2018.
- Nasjonal sikkerhetsmyndighet. *Grunnprinsipper*. Hentet 17.02.2026.

Dokumenter fra kommunen

- Rana brann og redning & Nesna brannvesen. *Risiko- og sårbarhetsanalyse Brann- og ulykkesrisiko*. Analyserapport. 17.01.2025.
- Rana brann og redning. *Evaluering Brann Tverrånesveien 5_23 okt*. Rapport. 23.10.2025.
- Rana brann og redning. *Evaluering/debrief støtteark*. Uten dato.
- Rana brann og redning. *Mal evalueringsskjema*. Evalueringsmal. Uten dato.
- Rana brann og redning. *Rana brann og redning 2026 øvingsplan*. Plan. Uten dato, oversendt 13.02.2026.
- Rana brann og redning. *Varmt RD_vaktlag A og foreb*. Evaluering. 05.11.2025.
- Rana kommune og Helgelandssykehuset. *Avtale om evakuering mellom elgelandssykehuset og Rana kommune*. Signert 11.06.2025.
- Rana kommune og Rana omsorgsberedskapsgruppe. *Samarbeidsavtale om beredskap mellom Rana kommune og Rana omsorgsberedskapsgruppe*. Signert 09.09.2025.
- Rana kommune og Røde Kors Rana. *Samarbeidsavtale om beredskap mellom Rana kommune og Rana Røde Kors*. Avtale. Signert 20.10.2021.
- Rana kommune, Hemnes kommune, Hattfjelldal kommune, Nesna kommune, Lurøy kommune, Træna kommune og Rødøy kommune. *Prosjekt: Interkommunal beredskapskoordinator Polarsirkelrådet 2025-2027*. Samarbeidsavtale. Uten dato.
- Rana kommune, Scandic Meyergården. *Samarbeidsavtale Scandic Meyergården Hotell og Rana kommune – Beredskapshotell*. Signert 07.08.2025.
- Rana kommune. *Atomberedskapsplan. Rana kommune 2024*. Plan. Vedtatt av SLG 23.05.2022. Endret administrativt 05.11.2024.
- Rana kommune. *Beredskapsplan Støttetjenesten 2025-2027*. Vedtatt og siste revidert av kommunaldirektør stab 15.10.2025.
- Rana kommune. *Beredskapsøvelse: Øvelse Nordland 2024*. Melding. Registrert 23.01.2024.

- Rana kommune. *Beredskapsøvelse: Øvelse Nordland 2025*. Melding. Registrert 29.01.2025.
- Rana kommune. *Beredskapsøvelser - gjennomføring av øvelse*. Rutine. Gyldig fra 19.05.2025.
- Rana kommune. *Evaluering av EKOM hendelser – 13.-14. desember 2025 og 27.-29. desember 2025 i Rana kommune*. 21.01.2026.
- Rana kommune. *Helhetlig risiko- og sårbarhetsanalyse RanaROS 2022-2025*. Analyserapport. Vedtatt av Kommunestyret 10.11.2022 sak 116/22.
- Rana kommune. *Helhetlig ROS (H-ROS)*. Rutine. Gyldig fra 03.10.2024.
- Rana kommune. *Kommunedelplan for byutvikling 2024-2034 Bestemmelser og retningslinjer*. Plan. Sist revidert 08.04.2025
- Rana kommune. *Ledelsens gjennomgang - Samfunnssikkerhet og beredskap 2024*. Notat. Behandlet i rådmannens strategiske ledergruppe (SLG) 10. november 2025.
- Rana kommune. *Overordnet beredskapsplan Rana kommune*. Plan. Vedtatt SLG 26.08.2024.
- Rana kommune. *Perspektivanalyse 2024-2027*. Analyse. Uten dato.
- Rana kommune. *Plan for brann og redning*. Plan. Godkjent 31.10.2025.
- Rana kommune. *Plan for krisekommunikasjon*. Plan. Gyldig fra 30.10.2025.
- Rana kommune. *Plan for opplæring og øvelser i helse og mestring*. Plan. Uten dato.
- Rana kommune. *Sektorplan beredskap for tekniske tjenester 2024-2027 Rana kommune*. Plan. Vedtatt av kommunaldirektør tekniske tjenester 20.9.2024.
- Rana kommune. *Sektorplan for beredskap i skoler og barnehager 2017-2018*. Vedtatt av utvalg for oppvekst og kultur 25.01.2017.
- Rana kommune. *Sektorplan: Beredskap for helse- og mestring 2023 – 2027*. Plan. Vedtatt av kommunestyret 20.05.2014, revidert og administrativt vedtatt 25.01.2023.
- Rana kommune. *Status oppfølgingstiltak – beredskap - november 2025 til ledelsens gjennomgang*. Oversikt. 06.11.2025.
- Rana kommune. *Varslingsplan Bydrift 2024 (HTML)*. Gyldig fra 26.06.2024.
- Rana kommune. *Varslingsplan bydrift 2024*. Plan. Gyldig fra 26.06.2024.
- Rana kommune. *Vedlegg 1 - Varslingsliste*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 10 - Loggføringsskjema*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 12 – Mal liaisonavtale*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 2 - Rutine kontaktpunkter og møteplasser for befolkning i bydeler og dalstrøk ved kriser*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 3 – Situasjonsrapportering*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 4 – Evakueringsplan 2024*. Vedlegg til overordnet beredskapsplan. Vedtatt av SLG 26.08.2024.
- Rana kommune. *Vedlegg 5 - Plan for opplæring og øvelser*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 6 – Beredskapsråd – Rana kommune*. Vedlegg til overordnet beredskapsplan. Uten dato.

- Rana kommune. *Vedlegg 7 – Tiltakskort kriseledelsen*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Vedlegg 9 - Evaluering*. Vedlegg til overordnet beredskapsplan. Uten dato.
- Rana kommune. *Årsregnskap og årsberetning 2024*. Rapport. Uten dato.

Andre kilder

- Statsforvalteren i Nordland. *Endelig rapport. Tilsyn med kommunal beredskapsplikt og helseberedskap. Rana kommune*. 24.08.2023.
- NRK, Telenor, Norkring og Norsk Lokalradioforbund. *Samarbeidsavtale om lokal- og riksradiostasjoners virksomhet under kriser og katastrofer*. Signert 2018.

Deloitte.