SALTEN KOMMUNEREVISJON

Forvaltningsrevisjon – Bodø kommune

Informasjonssikkerhet

September 2024

Forord

Salten kommunerevisjon IKS har på grunnlag av bestilling fra kontrollutvalget i Bodø kommune, engasjert Revisjon Midt-Norge SA til å gjennomføre forvaltningsrevisjon om informasjonssikkerhet i Bodø kommune. Denne rapporten oppsummerer resultatene fra forvaltningsrevisjonen.

Forvaltningsrevisjon er en pålagt oppgave etter kommunelovens § 23-2. Forvaltningsrevisjon innebærer å utføre systematiske undersøkelser av den kommunale tjenesteproduksjon, myndighetsutøvelse og økonomiske forvaltning, herunder se etter muligheter til forbedringer, eventuelt påpeke svakheter og mangler.

Salten kommunerevisjon IKS eies av kommunene Beiarn, Bodø, Fauske, Gildeskål, Hamarøy. Meløy, Saltdal, Steigen og Sørfold, og gjennomfører forvaltningsrevisjon innenfor en rekke områder. Vi har fire forvaltningsrevisorer med erfaringsbakgrunn fra både offentlig og privat virksomhet.

Salten kommunerevisjon IKS gjennomfører oppdragene i samsvar med NKRF – kontroll og revisjon i kommunene sin standard for forvaltningsrevisjon RSK 001. Krav til revisors uavhengighet følger av kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon. Salten kommunerevisjon IKS og Revisjon Midt-Norge SA har i forkant av og underveis i forvaltningsrevisjonen vurdert sin uavhengighet overfor Bodø kommune. Vi er ikke kjent med at det foreligger særegne forhold som er egnet til å svekke tilliten til vår uavhengighet og objektivitet.

Vi takker Bodø kommune for samarbeidet under undersøkelsen.

Bodø, 16.09.2024.

Margrete Haugum
Prosjektleder, forvaltningsrevisor

Bjørn Vegard Gamst
Oppdragsansvarlig forvaltningsrevisor

Innhold

Forord 2
Innhold 3
Sammendrag 6
1. Innledning 8
1.1 Formål og problemsstilling 8
1.2 Avgrensning av forvaltningsrevisjonen 8
1.3 Revisjonskriterier 8
1.4 Revidert enhet 9
1.5 Begreper 9
2. Metode 11
2.1 Bruk av kilder i rapporten 11
2.2 Kvalitetssikring og verifiseringsprosesser 13
3. Styringssystem for informasjonssikkerhet 14
3.1 Sikkerhetsstyring 14
3.1.1 Revisjonskriterium 14
3.1.2 Styringssystem i Bodø kommune 14
3.1.3 Revisors vurdering 17
3.2 Behandlingsoversikt 19
3.2.1 Revisjonskriterium 19
3.2.2 Behandlingsoversikt i Bodø kommune 19
3.2.3 Revisors vurdering 20
3.3 Internkontroll 20
3.3.1 Revisjonskriterium 20
3.3.2 Informasjonssikkerhet i kommunens internkontrollsystem 21
3.3.3 Revisors vurdering 22
3.3.4 Risikovurderinger i kommunen 22
3.3.5 Revisors vurdering 23
3.3.6 Personvernkonsekvenser 23
3.3.7 Revisors vurdering 23
3.3.8 Rutiner og prosedyrer 24
3.3.9 Revisors vurdering 24

3.3.10 Avvikssystem og avviksmeldinger 25
3.3.11 Revisors vurdering 25
3.3.12 Evaluere og lære av hendelser 26
3.3.13 Revisors vurdering 26
3.4 Opplæring av brukere 26
3.4.1 Revisjonskriterier 26
3.4.2 Opplæring 26
3.4.3 Revisors vurdering 28
3.5 Delkonklusjon 28
4. Tekniske og organisatoriske tiltak 29
4.1 Identifisere og kartlegge 29
4.1.1 Revisjonskriterier identifisere og kartlegge 29
4.1.2 Oversikt over enheter i IKT-systemet 29
4.1.3 Revisors vurdering 30
4.1.4 Oversikt over programvare 30
4.1.5 Revisors vurdering 30
4.1.6 Tilgangsstyring 31
4.1.7 Revisors vurdering 32
4.2 Beskytte og opprettholde 32
4.2.1 Revisjonskriterier beskytte og opprettholde 32
4.2.2 Anskaffelses- og utviklingsprosesser 33
4.2.3 Revisors vurdering 34
4.2.4 Ansvar for sikkerheten ved tjenesteutsetting 34
4.2.5 Revisors vurdering 35
4.2.6 Sikker IKT-struktur 36
4.2.7 Revisors vurdering 37
4.2.8 Sentral styring med sikkerhetsoppdateringer 37
4.2.9 Revisors vurdering 38
4.2.10 Plan for sikkerhetskopiering og ta sikkerhetskopier 38
4.2.11 Revisors vurdering 39
4.3 Oppdage sårbarheter, trusler og hendelser 39
4.3.1 Revisjonskriterier oppdage 39

4.3.2 Hva skal sikkerhetsovervåkes ... 39
4.3.3 Revisors vurdering ... 40
4.3.4 System for å overvåke sikkerheten ... 41
4.3.5 Revisors vurdering ... 42
4.4 Håndtere og gjenopprette ... 42
4.4.1 Revisjonskriterier håndtere og gjenopprette ... 42
4.4.2 Plan for hendelseshåndtering ... 42
4.4.3 Revisors vurdering ... 43
4.4.4 Plan for gjenoppretting ... 44
4.4.5 Revisors vurdering ... 44
4.5 Delkonklusjon ... 45
5. Oppsummering og konklusjon ... 46
6. Anbefalinger ... 47
7. Kommunedirektørens uttalelse ... 48
8. Referanser ... 50
9. Vedlegg ... 51
Vedlegg 1 – Kommunedirektørens uttalelse ... 51
Vedlegg 2 – Utledede revisjonskriterier ... 55
Vedlegg 3 – Sikkerhetsstrategier i Bodø kommune ... 64

Sammendrag

Revisjon Midt-Norge SA har på vegne av Salten Kommunerevisjon IKS gjennomført forvaltningsrevisjon om informasjonssikkerhet i Bodø kommune.

Kommunale dokumenter, intervjuer og en spørreundersøkelse til systemansvarlige i kommunen utgjør datagrunnlaget. Revisjonskriterier er hentet fra sikkerhetsloven, personopplysningsloven, eForvaltningsforskriften og virksomhetssikkerhetsforskriften. I tillegg er et utvalg av Nasjonal Sikkerhetsmyndighet sine grunnprinsipper for sikkerhetsstyring og IKT-sikkerhet lagt til grunn.

Den første problemstillingen er om Bodø kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

> *Revisor konkluderer med at Bodø kommune mangler et styringssystem for informasjonssikkerhet, som tilfredsstiller krav i regelverket.*

Revisjonen finner at sikkerhetsstyringen i kommunen omfatter fysisk sikkerhet og personellsikkerhet og i liten grad informasjonssikkerhet. Bodø kommune har et systematisk, men ikke formalisert arbeid med personvern (GDPR), blant annet med GDPR-gruppe og flere rutiner på områder, samt at det gjennomføres egenkontroller. Dette arbeidet kan betraktes som en del av arbeidet med informasjonssikkerhet, men er litt løsrevet fra sikkerhetsstyringen. Informasjonssikkerhet og personvern er to ulike fagområder som delvis overlapper hverandre.

Den andre problemstillingen som besvares er om Bodø kommune har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten.

> *Revisor konkluderer med at Bodø kommune ikke har tilfredsstillende organisatoriske og tekniske tiltak på plass for å ivareta informasjonssikkerheten.*

Når det mangler et helhetlig styringssystem for informasjonssikkerhet, mangler rammeverket for hvilke tekniske og organisatoriske tiltak som må på plass for å ivareta den informasjons-sikkerheten som kommunen ønsker å ha. Driftsavtalen som Bodø kommune har, ivaretar viktige områder på datasikkerhet, mens tekniske og organisatoriske tiltak på andre områder innenfor informasjonssikkerhet har liten oppmerksomhet eller er fraværende.

Når Bodø kommune kjøper tjenester til drift av informasjons- og kommunikasjonsteknologi krever det god bestillerkompetanse for å spesifisere hva de har behov for, samt for å følge opp driftsavtalen på et område som er i stadig utvikling. Når driftstjenestene kjøpes, kan det oppstå uavklarte forhold i grenseflaten mellom kommunen og driftsleverandøren.

Revisor anbefaler kommunedirektøren å vurdere følgende:

- Etablere et helhetlig styringssystem for informasjonssikkerhet.

- Sørge for å komplettere registrering av behandlingsprotokoller, herunder ferdigstille DPIAer og databehandleravtaler.
- Gi ansatte opplæring i informasjonssikkerhet.
- Gjennomgå driftsavtalen og følge den opp.
- Vurdere om tekniske og organisatoriske tiltak er i henhold til risikobildet og kommunens målsettinger for informasjonssikkerhet.

1. Innledning

1.1 Formål og problemsstilling

Kontrollutvalget i Bodø kommune bestilte en forvaltningsrevisjon om informasjonssikkerhet, slik det er beskrevet i revisors prosjektplan datert 17.11.2023. Kontrollutvalget fikk framlagt en revidert prosjektplan i møtet 07.03.3024, sak 12/24, hvor den framlagte prosjektplanen ble tatt til orientering.

Prosjektets formål er å finne ut om Bodø kommune har et tilfredsstillende system for regeletterlevelse på området informasjonssikkerhet. Dette belyses med følgende to problemstillinger:

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

Underveis i arbeidet er det gjort en språklig presisering i den første problemstillingen. Begrepet *helhetlig* er tatt inn i beskrivelsen av styringssystem, noe som er hentet fra eForvaltningsforskriftens § 15. Denne tilføyelsen medfører ingen substansiell endring av innholdet.

1.2 Avgrensning av forvaltningsrevisjonen

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

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

Bodø kommune er vertskommune for andre kommuner innenfor IKT. Disse er ikke omfattet av revisjonen.

1.3 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som revidert enhet skal vurderes 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 sikkerhetsloven, personopplysningsloven, e-forvaltningsforskriften og virksomhetssikkerhetsforskriften. I tillegg er Nasjonal sikkerhetsmyndighet (NSM) sine prinsipper for sikkerhetsstyring og IKT-sikkerhet lagt til grunn. Kriteriene er presentert innledningsvis under hvert tema. Utledningen av revisjonskriteriene følger som vedlegg to til rapporten.

Kriteriene er ikke nødvendigvis uttømmende for ethvert krav som stilles til alle sider av arbeidet innenfor området. Kriteriene er oppstilt etter revisjonens vurdering av hva som er det sentrale på området, basert på en vurdering av virksomhetens egenart og regelverket den forvalter. I tillegg er NSM sine prioritering av tekniske og organisatoriske tiltak[1] vektlagt.

1.4 Revidert enhet

Bodø kommune er revidert enhet. Det er hovedsakelig digitaliserings- og IKT-kontoret som er omfattet av revisjonen, men også andre deler av administrasjonsavdelingen. Digitaliserings- og IKT-kontoret er en del av administrasjonsavdelingen med assisterende kommunedirektør som avdelingsdirektør.

Det er ni ansatte på digitaliserings- og IKT-kontoret, opplyses det i oppstartsmøtet. I tillegg har digitaliserings- og IKT-kontoret prosjektstillinger, som er eksternt finansiert. Arbeidsoppgavene ved digitaliserings- og IKT-kontoret er:

- Forvaltning av IKT-plattformen inkludert systemansvar
- Avtaleforvaltning og leverandøroppfølging
- Utvikling og prosessforbedring
- Sikkerhet
- Eksternfinansierte prosjekter

Kommunen har mange skybaserte løsninger, men fortsatt noen lokale servere. Kommunen kjøper driftstjenesten gjennom en egen driftsavtale. Kommunen har i tillegg to egne konsulentavtaler, en om rådgiving på informasjonssikkerhet og en rammeavtale om IKT-utstyr. Kommunen er også medlem av HelseCert og KommuneCert.

Kommunen har et eget personvernombud som er organisert under assisterende kommunedirektør. Kommunen har en sikkerhets- og beredskapsrådgiver, som også er plassert i administrasjonsavdelingen.

1.5 Begreper

Informasjonssikkerhetsområdet inneholder mange forkortelse, engelske begreper og fremmedord. I rapporten er noen av begrepene erstattet med norske begrep, eksempelvis

[1] Støtteprodukter - Nasjonal sikkerhetsmyndighet (nsm.no)

brukes det sikkerhetskopi om backup. Under er noen av de sentrale begrepene forklart. Andre mer sporadisk brukte begreper er forklart i fotnote når de dukker opp.

IKT – informasjons- og kommunikasjonsteknologi

IT – informasjonsteknologi

Begrepene IKT og IT brukes i praksis om hverandre i dagligtale.

AD – active directory. Dette er betegnelsen på en katalogtjeneste levert av Microsoft, for håndtering av brukere, brukerrettigheter og ressurskontroll. (no.wikipedia.org/wiki/Active_Directory)

GDPR – general data protection regulation. Dette er en forkortelse for EUs personvernforordning. Den er en del av personopplysningsloven.

DPIA – data protection impact assessment. Dette er en risikovurdering av konsekvenser for personvernet.

Applikasjoner eller kortformen app – er et dataprogram.

2. Metode

Forvaltningsrevisjonsprosjektet er gjennomført i henhold til NKRF sin standard for forvaltningsrevisjon, RSK001. Standarden angir hva som er god kommunal revisjonsskikk innen forvaltningsrevisjon, og består av krav og anbefalinger knyttet til hvordan en forvaltningsrevisjon skal gjennomføres.

I henhold til standarden skal revisor innhente data i tilstrekkelig omfang til å kunne besvare prosjektets problemstillinger og å gjøre velbegrunnede vurderinger. Vi har derfor etterstrebet å benytte oss av ulike datakilder for å styrke rapportens pålitelighet og gyldighet. Det vil si å innhente data om samme forhold gjennom flere ulike metoder.

Revisor har hovedsakelig brukt dokumentstudier og intervjuer som kildemateriale, men har også samlet inn data gjennom en spørreundersøkelse blant systemansvarlig i kommunen. Samlet sett mener vi at datagrunnlaget gir et tilfredsstillende pålitelig og gyldig grunnlag for våre vurderinger og konklusjoner.

2.1 Bruk av kilder i rapporten

Sentrale dokumenter i forvaltningsrevisjonen er to styringsdokumenter med følgende tittel.

- Internkontroll og informasjonssikkerhet, styringssystem
- Internkontroll i Bodø kommune – «ORDEN I EGET HUS», styringsdokument

Revisor ønsker innledningsvis å gjøre oppmerksom på at disse to dokumentene lett kan forveksles ettersom de har lignende titler. Derfor brukes titlene på dokumentene når de omtales.

Andre sentrale dokumenter er rutinebeskrivelser og politiske saker. Bodø kommune har en GDPR-gruppe som blant annet gjennomfører egenkontroller. Revisor har benyttet rapporter fra egenkontrollene, referat fra møtene i GDPR-gruppen og annen intern informasjon, eksempelvis avviksstatistikk og utvalgte skjermdumper fra kvalitetssystemet og filsystemet.

Bodø kommune har en driftsavtale med en leverandør av driftstjenester. Driftsavtalen inneholder mange bestemmelser, som er relevant data i forvaltningsrevisjonen og er benyttet som datakilde.

Den skriftlige dokumentasjonen som er innhentet er et utvalg av de dokumenter som revidert enhet mener er relevant. I tillegg har revisor etterspurt andre dokumenter og fått disse tilsendt. Revisor har erfart at dokumentasjon av rutiner er spredt i organisasjonen og alt er ikke samlet i kvalitetssystemet. Det betyr at det kan finnes relevante dokumenter som revisor ikke har klart å finne fram til eller fått tilsendt.

Det ble gjennomført et digitalt oppstartsmøte med kommunedirektør, assisterende kommunedirektør og digitaliserings- og IKT-sjef. Videre er det gjennomført stedlige intervjuer med følgende roller i organisasjonen.

- Digitaliserings- og IKT-sjef
- Personvernombudet
- Sikkerhets- og beredskapsrådgiver
- Seniorrådgiver digitaliserings- og IKT-kontoret
- Service- og arkivleder
- Digital løsningsdesigner
- Rådgiver/ digital løsningsdesigner
- Rådgiver ForUt (forvaltnings- og utviklingsteam)
- Ingeniør, teknisk og eiendomsavdelingen
- Rådgiver, oppvekst og kulturavdelingen
- Rådgiver, kvalitetskoordinator

I forkant av de stedlige intervjuene ble det laget en felles strukturert intervjuguide. Revisors kontaktperson i kommunen hadde booket intervjuer på forhånd med de som vedkommende mente burde intervjues. Revisor ba om et intervju i tillegg til de som var oppsatt. Flere av de som ble intervjuet er medlemmer i kommunens GDPR-gruppe (omtales nærmere i 3.2.2). Dette innebar at ulike deler av intervjuguiden var relevant for de som ble intervjuet.

Det er skrevet referat fra alle intervjuene og disse er godkjent. I tillegg har noen av de som ble intervjuet fått oppfølgingsspørsmål på epost, og revisor har også etterspurt og fått tilsendt noe dokumentasjon som ble nevnt i intervjuene.

Det er en svakhet at revisor hadde liten innvirkning på hvem som ble intervjuet. Det ble supplert med en ansatt ut over de som kontaktpersonen hadde gjort intervjuavtaler med. Hadde revisor valgt ut intervjuobjekter selv, ville nok utvalget vært annerledes. Samtidig bidro alle de utvalgte med relevant informasjon til revisjonen. Det ble vurdert å gjennomføre flere intervjuer digitalt, for å øke tilfanget av intervjuobjekter. Vurderingen endte med at datatilfanget vi fikk fra de stedlige intervjuene var tilstrekkelig, fordi det representerte ulike perspektiver på informasjonssikkerhet.

Under intervjuene kom det fram at kommunen har mange systemansvarlige. Det ble besluttet å gjennomføre en kort elektronisk spørreundersøkelse (14 spørsmål) til systemansvarlige, med blant annet spørsmål om tilganger, registrering i Digiorden[2] og oppdateringer. Kommunen sendte over en liste med 39 systemansvarlige som ble lagt til grunn. Flere av de systemansvarlige har ansvar for flere systemer og de ble bedt om å velge seg ett system å svare ut fra. Det var 25 som gjennomførte hele undersøkelsen, noe som gir en svarprosent på 64. Det vurderes i utgangspunktet å være tilfredsstillende. Denne svarprosenten indikerer at

[2] Digiorden er en applikasjon (dataprogram) som er et styringssystem for informasjonsforvaltning.

resultatene til en viss grad er generaliserbare. Undersøkelsen er ikke bygd opp slik at det er mulig å undersøke eventuelle skjevheter i datamaterialet. Det er også en svakhet i dataene at en systemansvarlig som har ansvar for flere systemer, kan svare ulikt for ulike systemer. Dette fanges ikke opp i spørreundersøkelsen.

Spørreundersøkelsen ble sendt ut 25.06.2024 med svarfrist 02.07.2024. Det ble sendt en påminnelse før fristen og det ble sendt en purring. Undersøkelsen ble avsluttet 04.07.2024. Det er gjennomført en enkel analyse av dataene i spørreundersøkelsen. Vi kan anta at en forklaring på forskjeller i datamaterialet kan ha sammenheng med hvor mange systemer den enkelte har systemansvar for. Bakgrunnen for dette er at ansatte er mer kjent med oppgaver som gjøres ofte enn de som gjøres en gang i blant.

2.2 Kvalitetssikring og verifiseringsprosesser

Denne forvaltningsrevisjon er gjennomført og kvalitetssikret etter kravene i RSK 001 og Salten kommunerevisjons interne kvalitetssikringssystem for forvaltningsrevisjon.

Rapporten er kvalitetssikret av prosjektleder og prosjektmedarbeider ved Revisjon Midt-Norge SA sammen med oppdragsansvarlig forvaltningsrevisor ved Salten kommunerevisjon IKS.

Etter avtale med kommuneledelsen i oppstartsmøtet er utkast til rapport oversendt kommunen 15.08.2024, for

- faktaverifisering av datadelen av rapporten, med en egen tilbakemelding.
- kommunedirektørens uttalelse, med en høringsuttalelse som i sin helhet vedlegges rapporten i vedlegg en.

Revisor mottok en tilbakemelding på faktaverifiseringen 29.08.2024 og har rettet opp to konkrete feil som var avdekket. Behandlingen av kommunedirektørens uttalelse framgår i kapittel sju.

3. Styringssystem for informasjonssikkerhet

Den første problemstillingen er om Bodø kommune har etablert et helhetlig styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket. Denne problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet.

Problemstillingen ser på om kommunen har vurdert hvilke informasjonsverdier kommunen har, hvilke trusler som finnes og hvor sårbar kommunen er hvis denne informasjonen ikke blir tilgjengelig eller kommer på avveie. Revisor vil se på om informasjonssikkerhet er en del av kommunens internkontrollsystem, uten at det er en revisjon av internkontrollen i kommunen. En del av problemstillingen er å se om kommunen ivaretar personopplysninger i tråd med krav i regelverket. Revisjonskriteriene er utledet i vedlegg to.

3.1 Sikkerhetsstyring

3.1.1 Revisjonskriterium

- Kommunen skal ha et styringssystem for sikkerhet som omfatter informasjonssikkerhet, som angir
    - Sikkerhetsmål
    - Sikkerhetsstrategi
    - Sikkerhetsorganisasjon, hvor roller og ansvar framgår.

3.1.2 Styringssystem i Bodø kommune

Kommunen har et styringsdokument for informasjonssikkerhet og GDPR som heter *internkontroll og informasjonssikkerhet, styringssystem*. Dokumentet er ikke datert, men i et av intervjuene opplyses det at dokumentet ble utarbeidet i 2018-2019. En annen forteller at dokumentet skulle vært revidert i 2022, men at revisjonen er utsatt til 2025. En skjermdump fra kommunens kvalitetssystem viser at dokumenter er opprettet der 04.12.2018, endret 15.04.2021, revidert 15.04.2024 og neste revisjon er 15.04.2025. Av skjermdumpen går det fram at det er administrasjonsavdelingen, sikkerhet og beredskap, ved sikkerhets- og beredskapsrådgiver som har ansvaret.

I oppstartsmøtet fortelles det at arbeidet med informasjonssikkerhet er godt beskrevet i dokumentet internkontroll og informasjonssikkerhet, og at deler av dokumentet er godt implementert, mens andre deler er veldig dårlig implementert. Det komplette styringssystemet mangler, og arbeidet med informasjonssikkerhet er noe oppstykket og delt i kommunen. Kommunen må velge standarder for informasjonssikkerhet ut fra forsvarlig ressursbruk i forhold til andre enheter i kommunen, fortelles det i oppstartsmøtet. Dette utdypes med at kommunen har fokusert på de viktigste områdene, og innenfor informasjonssikkerhet har det vært det operative. Digitaliserings- og IKT-sjefen opplyser at kommunens driftsavtale regulerer datasikkerheten.

Flere av de som er intervjuet nevner også kommunens digitaliseringsstrategi, men at denne er overfladisk og handler lite om informasjonssikkerhet.

Sikkerhetsmål

Det framgår av dokumentet internkontroll og informasjonssikkerhet at Bodø kommunes overordnede sikkerhetsmål er å opprettholde konfidensialitet, integritet og tilgjengelighet for all behandling av personopplysninger.

Kommunens personvernerklæring oppgir følgende sikkerhetsmål:

- Opplysningene skal være tilgjengelige for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring.
- Opplysningene skal behandles i tråd med reglene om taushetsplikt og være beskyttet, slik at uvedkommende ikke får kjennskap til dem.
- Opplysningene skal være fullstendige, oppdaterte og korrekte og et resultat av lovlige registreringer og kontrollerte aktiviteter.
- Opplysningene skal begrenses, slik at det kun er dokumentert tjenstlige behov som utløser tilgang.

I intervjuene er det få som har noe forhold til sikkerhetsmålene. Digitaliserings- og IKT-sjefen forteller at sikkerhetsmålene i dokumentet internkontroll og informasjonssikkerhet er et utgangspunkt. Målene er på makronivå og må innfris lengre ned i organisasjonen.

Sikkerhetsstrategi

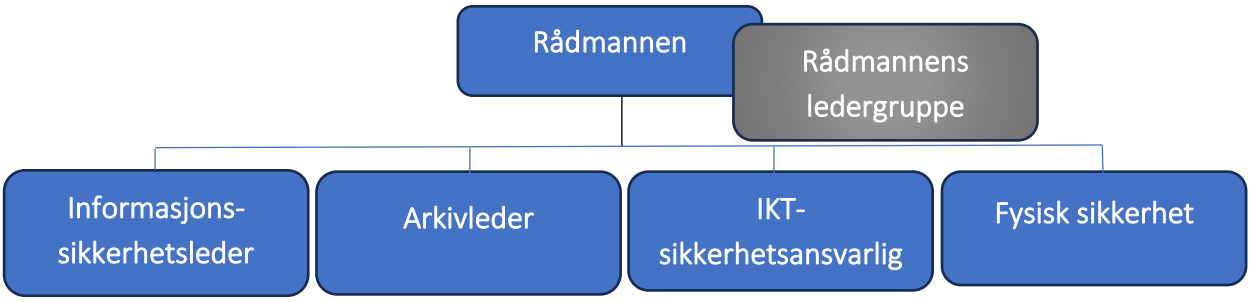
Kommunens strategi for å nå sikkerhetsmålene og sikre etterlevelse av lover, forskrifter og interne retningslinjer er listet opp i 24 punkter i dokumentet internkontroll og informasjonssikkerhet. Revisor har valgt å gi tre eksempler her og den komplette listen finnes i vedlegg tre.

- Forebygge uautorisert innsyn i IT-systemene og i annen informasjon ved tilsiktede handlinger som tyveri, hacking, virusspredning osv.
- Informasjonssikkerhetsarbeidet i Bodø kommune skal være et kontinuerlig forbedringsarbeid underlagt et systematisk og planlagt styringssystem.
- Kommunen skal opptre proaktivt og etablere alle nødvendige og organisatoriske og tekniske tiltak for å sikre at regelverket etterleves.

Det er få av de som ble intervjuet som har et forhold til sikkerhetsstrategien. Digitaliserings- og IKT-sjefen forteller at kommunen jobber godt med den og har kommet langt i å etterleve den.

Sikkerhetsorganisasjon

Sikkerhetsorganisasjonen beskrives i dokumentet internkontroll og informasjonssikkerhet, styringssystem. Her henvises det til et organisasjonskart som er gjengitt under i figur 1.



Kilde: Bearbeidet versjon hentet fra Internkontroll og informasjonssikkerhet, Bodø kommune, udatert.

Figur 1: Sikkerhetsorganisasjonen i Bodø kommune.

Sikkerhetsorganisasjonen er forklart med at kommunen er behandlingsansvarlig og rådmannen har det øverste administrative ansvaret for informasjonssikkerheten i Bodø kommune.

RLG er rådmannens ledergruppe og består av kommunaldirektørene i tillegg til rådmannen[3]. Kommunaldirektørene har det daglige, operative ansvaret for informasjonssikkerheten i egen avdeling. Dette omfatter blant annet å ha en oppdatert behandlingsoversikt, sørge for at databehandleravtaler er signert og følge opp og behandle avvik.

Videre er følgende roller beskrevet:

- Informasjonssikkerhetsleder – pådriver og koordinator i informasjonssikkerhetsarbeidet.
- IKT-sikkerhetsansvarlig – overordnet ansvar for koordinering, rådgiving og kontroll av IKT-sikkerhetsarbeidet i kommunen.
- Ansvarlig fysisk sikkerhet – ansvar for fysisk sikring av inn- og utearealer til kommunens ulike lokasjoner og bygninger.
- Sikkerhetsutvalg – rådgivende organ i spørsmål relatert til informasjonssikkerhet.
- Systemeier – ansvarlig for å utvikle, forvalte og drifte informasjonssystem i Bodø kommune.
- Systemansvarlig – systemeiers ressurs for å gjennomføre nødvendige konfigureringer i systemet.
- Personvernombud – rådgiver innenfor personvern og veilede om forpliktelser etter personvernlovgivingen

I oppstartsmøtet fortelles det at digitaliserings- og IKT-kontoret er representert i kommunens ledergruppe ved assisterende kommunedirektør. Digitaliserings- og IKT-sjefen deltar ved behov. De ulike avdelingsdirektørene er systemeiere og har det formelle ansvaret for sikkerhet i systemene de eier.

[3] Dokumentet er fra 2018 og da brukte kommunen betegnelsene rådmann og kommunalsjefer, mens de samme rollene i dag heter kommunedirektør og avdelingsledere.

Kommunen har en tverrsektoriell gruppe som jobber med GDPR, opplyses det i oppstarts-møtet. Gruppen fører internt tilsyn med kommunen. Flere av de som er intervjuet er medlemmer i denne gruppen, men flere sier at denne gruppen ikke er en del av sikkerhets-organisasjonen slik den er beskrevet i dokumentet internkontroll og informasjonssikkerhet. GDPR-gruppen har ikke noe formelt mandat og har en uklar myndighet, forteller flere i intervjuene. En uttrykker at GDPR-gruppen dekker sikkerhetsutvalget til en viss grad. Det er ikke fokus på informasjonssikkerhet, men på GDPR. En annen forteller at GDPR-gruppen sine oppgaver hovedsakelig er å revidere rutiner og prosedyrer samt å gjennomføre egenkontroller. I tillegg svarer gruppen på henvendelser fra organisasjonen. En uttrykker at GDPR-gruppen fungerer bra, men at gruppens arbeid ikke er godt nok forankret på ledernivå.

Digitaliserings- og IKT-sjefen forteller at kommunen ikke har noen informasjonssikkerhets-leder. Digitaliserings- og IKT-sjefen har det formelle ansvaret for IKT-sikkerhet og har en medarbeider som fungerer som sikkerhetsrådgiver. Ansvar og myndighet til sikkerhetsrådgiver skal tydeliggjøres i delegeringsreglementet som er under revisjon.

I dagens delegeringsreglement er bestemmelsene i sikkerhetsloven, eksempelvis § 4-1 sikkerhetsstyring og § 4-3 plikt til å gjennomføre sikkerhetstiltak, delegert til assisterende kommunedirektør. Det er ingen delegeringer knyttet til personopplysningsloven.

En av de ansatte ved digitaliserings- og IKT-kontoret forteller at vedkommende sitt arbeid er knyttet til datasikkerhet. Det omhandler blant annet om brannmurer, serverpark, nettverk og jevnlige kontroller av systemene, mens informasjonssikkerhet er mer omfattende enn dette. Vedkommende forteller at det er systemeierne som må ta ansvar for informasjonssikkerheten.

Flere forteller at det er opprettet en arbeidsgruppe for fysisk sikkerhet, som i juni 2024 har fått mandat fra kommunedirektøren. Gruppen ledes av sikkerhets- og beredskapsrådgiver, som har ansvar for fysisk sikkerhet og personellsikkerhet. Vedkommende er i staben til assisterende kommunedirektør. I oppstartsmøtet fortelles det at sikkerhet- og beredskapsrådgiver har et bredt ansvar og en nøkkelrolle i sikkerhetsarbeidet. Sikkerhets- og beredskapsrådgiver forteller at vedkommende har ansvaret for det overordnede sikkerhetsarbeidet i kommunen og er ansvarlig for personell og fysisk sikkerhet, men ikke informasjonssikkerhet.

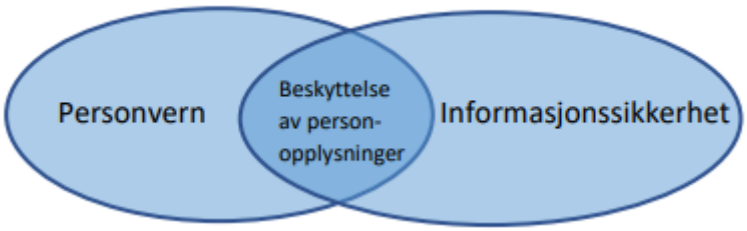
3.1.3 Revisors vurdering

Revisjonskriteriet sier at kommunen skal ha et styringssystem for sikkerhet som omfatter informasjonssikkerhet, som angir sikkerhetsmål, sikkerhetsstrategi og en sikkerhetsorganisasjon, hvor roller og ansvar framgår.

Revisor vurderer at Bodø kommune ikke har noe operativt styringssystem for informasjonssikkerhet med sikkerhetsmål, sikkerhetsstrategier og en sikkerhetsorganisasjon.

Kommunens dokument internkontroll og informasjonssikkerhet, beskriver et styringssystem for informasjonssikkerhet med vekt på GDPR. Dokumentet ble laget i 2018 og har ikke blitt vesentlig revidert senere og er heller ikke implementert i kommunen.

Målsettingen som angis i styringsdokumentet er knyttet til personopplysninger. Figuren under er hentet fra KS og KPMG sitt dokumentet *kommunedirektørens verktøykasse for personvern og informasjonssikkerhet,* og det viser sammenhengen mellom personvern og informasjonssikkerhet. I tilknytning til figuren står det at informasjonssikkerhet og personvern er to ulike fagområder, men overlapper når det gjelder beskyttelse av personopplysninger.



Kilde: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, udatert, KS og KPMG

Figur 2. Sammenhengen mellom informasjonssikkerhet og personvern.

Dokumentet internkontroll og informasjonssikkerhet angir 24 strategier, men utfordringen er at de ansatte ikke har noen forhold til verken dokumentet eller strategiene.

Den sikkerhetsorganisasjonen, med roller og ansvar, som beskrives i styringsdokumentet er ikke operativ. Sikkerhets- og beredskapsrådgiver har fått et ansvar for fysisk sikkerhet og personell sikkerhet, men mangler informasjonssikkerhet. Den delen av informasjonssikkerhet som gjelder beskyttelse av personopplysninger ivaretas til en viss grad av GDPR-gruppen. Utfordringen er at GDPR-gruppen ikke har noen formell forankring og mandat i kommuneorganisasjonen. Digitaliserings- og IKT-sjefen uttaler å ha ansvaret for cybersikkerheten og sørge for at IKT-løsninger er i et sikkert miljø. En av lederne på digitaliserings- og IKT-kontoret har ansvaret for datasikkerheten. Revisor oppfatter at ansvaret for informasjonssikkerhet blir fragmentert og at organiseringen med GDPR-gruppen og sikkerhets- og beredskapsrådgiver, som nylig har opprettet en gruppe for fysisk sikkerhet, kan føre til at informasjonssikkerhet faller mellom disse to gruppene. Det kommer også fram uklare forventinger til sikkerhets- og beredskapsrådgiverens ansvar.

Når flere henviser til at det er systemeierne (avdelingsdirektørene) som må ta ansvaret for informasjonssikkerheten, viser dette at informasjonssikkerhetsarbeidet ikke er forankret i kommunens ledelse. Dette underbygges av at delegeringsreglementet ikke sier noe om slik delegering fra kommunedirektøren til kommunalsjefene.

3.2 Behandlingsoversikt

3.2.1 Revisjonskriterium

- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.

3.2.2 Behandlingsoversikt i Bodø kommune

I kommunens dokument for internkontroll og informasjonssikkerhet er en av sikkerhetsstrategiene at forholdet mellom behandlingsansvarlig og databehandler skal være regulert i en databehandleravtale, som skal sikre at personopplysninger blir behandlet i samsvar med regelverket. Dette gjelder både der kommunen er behandlingsansvarlig, men også når kommunen er databehandler.

I intervjuene fortelles det at databehandleravtaler finnes i Digiorden. I følge flere som ble intervjuet er ikke alle systemene (applikasjonene) registrert i Digiorden. Behandlingsoversiktene er lagt inn for hvert system, men det er slik at behandling av personopplysninger kan gjøres i flere systemer som er integrert. Bodø kommune har en egen rutine for bruk av Digiorden, som sier at alle datasystemer skal registreres i Digiorden, og for systemer som inneholder personopplysninger skal det opprettes datasett[4] og behandlingsprotokoll. Det opplyses at det er utarbeidet en brukerveiledning for hvordan applikasjoner skal registreres i Digiorden. De systemansvarlige får tilgang til denne brukerveiledningen. Informasjon om utfylling av behandlingsprotokoll ligger inne i rutinen. I rutinen opplyses det at utfylt behandlingsprotokoll genererer en personvernerklæring for hver enkelt behandling og behandlingene knyttes opp mot det datasettet hvor behandlingene foregår om den skjer i en applikasjon. Rutinene gir også noen føringer for rollen som systemansvarlig.

Oversikten over alle registrerte systemer viser 197 systemer. I denne oversikten er det blant annet lagt inn lenker til databehandleravtale for 61 systemer. Den eldste er inngått i 2016 og tre databehandleravtaler er inngått i 2024. Revisor har fått oversendt oversikt over behandlingsprotokoller som viser at 136 systemer er registrert. Dette er systemer hvor det finnes personopplysninger. Av disse systemene er 84 ferdig registrert, mens 12 systemer ligger inne med bare malen. For 41 av systemene er det ikke opplyst om internt ansvarlig. Spørreundersøkelsene til de systemansvarlige viser at 96 prosent av de som har svart, har fullført registreringen.

Revisor har også fått eksempel på ferdig utfylt behandlingsprotokoll, delvis utfylt og malen for behandlingsprotokoll. Behandlingsprotokollen er bygd opp etter bestemmelser i personopplysningsloven med referanse til bestemmelsene.

[4] Datasett – er en betegnelse på data (innholdet) som legges inn i en applikasjon/program.

En av de ansatte forteller at kommunen har en egen mal for databehandleravtaler, men at vedkommende foretrekker å bruke leverandørens mal slik at ikke noe glipper. Vedkommende bistår med å kvalitetssikre databehandleravtalene, mens det er systemansvarlig som signerer. En av de ansatte mener at de tidligere databehandleravtalene ikke holder mål juridisk for kommunen og at det er behov for å tydeliggjøre ansvaret. (Revisor har ikke undersøkt avtalene.) Vedkommende mener at Digiorden ikke er god nok og ønsker blant annet en utfyllende informasjon om formål og hensikt med registreringene i systemene.

Det er systemansvarlige som har ansvaret for å gjøre registreringene i Digiorden. En forteller at det er ulikt hvordan Digiorden brukes og det er mye opp til systemeier. En annen forteller at det er tidkrevende å bruke Digiorden.

3.2.3 Revisors vurdering

Revisjonskriteriet sier at kommunen skal føre protokoll over hvilke personopplysninger de behandler.

> *Revisor vurderer at Bodø kommune har et system, Digiorden, for å føre protokoll over hvilke personopplysninger de behandler, men registreringene er ikke fullstendig.*

Revisor finner at ansvaret for å føre behandlingsprotokollene er fordelt utover i organisasjonen på minst 39 systemansvarlige. I oversikten er det ikke oppgitt hvem som er ansvarlig for alle systemene. Det er positivt at det er laget en rutine samt en egen veiledning for registreringer i Digiorden. Det er kritikkverdig at alle registreringene ikke er på plass. Det ser ut til å være avvik mellom at 96 prosent av de systemansvarlige svarer at de har fullført registreringen, mens det i Digiorden er fullført registrering av 84 av 136 systemer. Dette kan muligens forklares med at det er de som har svart på spørreundersøkelsen, som har registrert sine systemer. I tillegg kan det være slik at disse respondentene har ansvar for flere systemer og at de har svart ut fra et bestemt system og at dette systemer er registrert full ut.

3.3 Internkontroll

3.3.1 Revisjonskriterium

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- Kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.

- Kommunen må ha et avvikssystem og ansatte må melde avvik.
- Kommunen bør evaluere og lære av hendelser.

3.3.2 Informasjonssikkerhet i kommunens internkontrollsystem

Bodø kommune har et styringsdokument for internkontroll i Bodø kommune – «ORDEN I EGET HUS». Dokumentet er vedtatt i kommunedirektørens ledermøte 07.02.2022 og versjon 2 er vedtatt i kommunedirektørens ledergruppe 11.12.2023. I styringsdokumentet for internkontroll står det at Bodø kommune skal ha ulike sektorovergripende dokumenter. Deriblant informasjons- og datasikkerhet og prosedyrer for håndtering av personopplysninger (GDPR) og sikkerhet og beredskap. Blant dokumenter som avdelingene/virksomhetene skal ha på plass er beredskapsplaner- og prosedyrer. Revisor har fått tilsendt oversikt over prosedyrer for håndtering av personvernopplysninger. Revisor har ikke funnet noe sektorovergripende dokument for informasjons- og datasikkerhet.

Styringsdokumentet for internkontroll beskriver fire hovedområder for risikovurderinger/ internkontroll. Det er

- Virksomhetenes kjerneaktivitet/tjenesteleveranse
- HMS
- GDPR
- Sikkerhet og beredskap

For de tre siste områdene skal fokus være på risikoen for ikke å etterleve kommunens og virksomhetenes gjeldende prosedyrer og retningslinjer, samt håndtering av uønskede hendelser.

I årsmeldingen for 2023 rapporteres det fra internkontrollarbeidet i Bodø kommune. Det opplyses at det brukes sjekklister i rapporteringssystemet som virksomhetene rapporterer på, men at svarprosenten i 2023 ikke er stor nok til å få en betryggende kontroll. Det rapporteres om styringsdokumenter for internkontroll og kommunens HMS-plan følges. Sjekklistene gjenspeiler hovedelementene i kommunens internkontrollsystem.

En av sikkerhetsstrategiene i dokumentet internkontroll og informasjonssikkerhet, er at informasjonssikkerhetsarbeidet i Bodø kommune skal være et kontinuerlig forbedringsarbeid underlagt et systematisk og planlagt styringssystem.

En av de ansatte forteller at egenkontrollene som GDPR-gruppen gjennomfører bidrar til bedre internkontroll i ulike deler av kommunen. De finner at mange rutiner og prosedyrer er på plass, men at praksisen varierer. I dokumentet internkontroll i Bodø kommune beskrives egenkontroll og at denne initieres av internkontrollgruppen.

3.3.3 Revisors vurdering

Revisjonskriteriet er at informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

> *Revisor vurderer at informasjonssikkerhet er en planlagt del av internkontrollen i Bodø kommune, men at det mangler et sektorovergripende dokument for informasjons- og datasikkerhet.*

Vurderingen er basert på at sektorovergripende dokumenter mangler og at sjekklistene som skal gjenspeile hovedelementene i internkontrollsystemet har lav svarprosent, slik at praksisen heller ikke ivaretar informasjonssikkerhet i internkontrollen. GDPR-gruppens praksis med egenkontroller kan betraktes som en internkontroll, men denne er lite forankret i kommunens internkontrollsystem som snakker om egenkontroller initiert av internkontrollgruppen.

3.3.4 Risikovurderinger i kommunen

Bodø kommune har en overordnet ROS-analyse fra 2018 med en tilhørende beredskapsplan. I ROS-analysen er bortfall av IKT-infrastruktur, samt bortfall av elektronisk kommunikasjon vurdert. Følgende beredskapstiltak ligger i planen:

- Etablere manuelle rutiner for utføring av viktige oppgaver dersom tele og IT faller bort.
- Nødstrøm
- Databehandleravtaler
- Bygge redundante løsninger for drift av kritiske tjenester
- Utarbeide konfigurasjonsoversikt
- Utarbeide beredskapsplan IKT
- Utarbeide ROS-analyse IKT

Både overordnet ROS-analyse og beredskapsplan er under revidering, fortelles det i oppstartsmøtet. I ROS-analyse er ikke hendelser rundt informasjonssikkerhet inkludert som en egen uønsket hendelse, bortsett fra hacking. I oppstartsmøtet fortelles det at informasjonssikkerhet og bortfall av for eksempel IKT kan være følgehendelser og en konsekvens av andre uønskede hendelser i ROS-analysen. Kommunen gjennomførte en intern øvelse på bortfall av IKT for noen år siden.

ROS-analyser gjøres hver gang det gjøres anskaffelser av en viss betydning og tilsvarende, fortelles det i oppstartsmøtet.

En av sikkerhetsstrategiene i dokumentet internkontroll og informasjonssikkerhet er at risikovurderinger skal brukes aktivt for å forbedre de tekniske og organisatoriske tiltakene i informasjonssystemene. Risikovurderinger gjøres i kvalitetssystemet. Det finnes en egen prosedyre for ROS-analyse med mål om å forebygge avvik og uønskede hendelser knyttet til

blant annet systemer, prosesser og aktiviteter. Prosedyrer gjelder for alle nivå i organisasjonen og ansvaret ligger til lederne på alle nivå. ROS-analysene skal dokumenteres i kvalitetssystemet. I tillegg skal ROS-analysen arkiveres i sak- og arkivsystemet, hvis den er knyttet til en sak eller en beslutning. Sektorovergripende risikovurderinger gjennomføres på eget skjema og lagres i sak- og arkivsystemet. Det finnes også en prosedyre for risikoakseptkriterier, med formål å etablere en standard for hvor mye risiko kommunen kan akseptere i forbindelse med behandling av personopplysninger og informasjonssikkerhet.

For 11 av de 197 applikasjonene som ligger i Digiorden er det registrert ROS-analyse.

3.3.5 Revisors vurdering

Revisjonskriteriet er at kommunen regelmessig skal gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.

> *Revisor vurderer at kommunen gjennomfører risikovurderinger, men i for lite omfang til at det gir et grunnlag for informasjonssikkerhetstiltak.*

Revisor finner at flertallet av de systemene som er registrert i Digiorden mangler risikovurderinger. Systemet og planen for å gjennomføre risikoanalyser finnes, men det er i liten grad gjennomført.

3.3.6 Personvernkonsekvenser

En av sikkerhetsstrategiene i dokumentet internkontroll og informasjonssikkerhet er å sørge for at det foretas tilfredsstillende vurdering av personvernkonsekvenser (DPIA) ved innføring av nye informasjonssystemer.

En av de som arbeider med utvikling av nye systemer, forteller at vedkommende holder på å lage en full prosessbeskrivelse for innføring av nye systemer, samt rutinebeskrivelser hvor DPIA inngår. Det opplyses at det lages DPIA ved anskaffelser av en viss betydning. Det er utarbeidet flere DPIAer, spesielt innenfor helse. I Digiorden er det en egen kolonne for DPIA, men det er ikke registrert noen DPIAer der. I spørreundersøkelsen oppgir 70 prosent at de har vurdert personvernkonsekvenser, mens 11 prosent har ikke gjort noen vurdering. Det finnes en mal for gjennomføring av DPIA, som revisor har fått tilsendt.

Revisor har fått en presentasjon som viser prosessen omkring DPIA for utekontaktens bruk av Snapchat med ungdommer, samt selve DPIAen som er utfylt etter den malen kommunen har. Snapchat er ikke et av systemene som ligger inne i Digiorden.

3.3.7 Revisors vurdering

Revisjonskriteriet er at kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

Revisor vurderer at personvernkonsekvenser vurderes, men det mangler dokumentasjon på det.

Ifølge spørreundersøkelsen har 70 prosent av de systemansvarlige vurdert personvernkonsekvenser, mens det ikke registrert noen i Digiorden. Revisor har ikke funnet noen forklaring på forskjellene her. Revisor har fått dokumentasjon på kun en vurdering av personvernkonsekvenser (DPIA). Kommunen har en mal for vurdering av personvernkonsekvenser, noe som er nyttig for å bidra til å gjennomføre vurderingen.

3.3.8 Rutiner og prosedyrer

I styringsdokumentet for internkontroll i Bodø kommune går det fram at prosedyrer, retningslinjer og reglement er i et dokumentbibliotek i kvalitetssystemet. Nødvendige prosedyrer opprettes, lagres og revideres slik at de er gjenfinnbare for alle ansatte. Det er virksomhetslederen som har ansvaret for at nødvendige prosedyrer opprettes og vedlikeholdes, samt å sikre at de blir fulgt og fungerer etter hensikten. Alle ansatte skal ha tilgang til kvalitetssystemet.

I intervjuene opplyses det at det finnes en del rutiner og prosedyrer for informasjonssikkerhet i kvalitetssystemet. Noe av dette ligger åpent, da det er felles med andre kommuner som Bodø kommune er vertskommune for. Revisor har fått oversikt over prosedyrer som ligger i kvalitetssystemet under GDPR. Disse er delt i styrende, gjennomførende og kontrollerende rutiner med til sammen 18 dokumenter. I tillegg finnes det flytskjema for prosesser som er lagret på digitaliserings- og IKT-kontoret sitt eget filområde og ikke i kvalitetssystemet.

En forteller at det er flere rutiner på GDPR, men vedkommende har inntrykk av at de er lite brukt. En annen forteller at kommunen ikke er flink til å bygge opp overgripende rutiner, men gode på enkeltområder.

3.3.9 Revisors vurdering

Revisjonskriteriet er at kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.

Revisor vurderer at kommunen har noen rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser, men at disse i hovedsak er knyttet til GDPR.

Revisor finner at ikke alle rutiner og prosedyrer er samlet i kvalitetssystemet, men at eksempelvis digitaliserings- og IKT-kontoret har prosedyrer på eget filområde. Det er revisors inntrykk at rutiner og prosedyrer i kvalitetssystemet er mangelfulle, spesielt for informasjonssikkerhet.

3.3.10 Avvikssystem og avviksmeldinger

Avvikssystemet er beskrevet i styringsdokumentet for internkontroll i Bodø kommune og at dette er et elektronisk kvalitetssystem. Avvik skal meldes til og behandles av nærmeste leder. Opplæring innenfor avvik er nærmeste leders ansvar.

En av sikkerhetsstrategiene i dokumentet internkontroll og informasjonssikkerhet er at alle avvik og sikkerhetsbrudd skal registreres i kvalitetssystemet for oppfølging, korrigering og forbedring.

I årsmelding for 2023 er det rapportert om totalt 8314 avvik i kommunen. Av disse er 148 registrert som GDPR-avvik. For perioden 2020 til 2023 er det registrert 488 GDPR-avvik og 87 avvik første halvår 2024. Avvikskategoriene for GDPR er gitt i listen under, samt den prosentvise fordelingen for perioden 2020-2023.

- Brudd på registrertes rettigheter – 4,4 prosent. (Feilaktig håndtering av anmodninger, manglende melding ved sikkerhetsbrudd, personopplysninger oppbevart lengre enn beskrevet i formål, annet – brudd på de registrertes rettigheter)
- Forholdet til tilsynsmyndigheten - 0. (Avvik/merknad fra Datatilsynet)
- Personopplysninger på avveie 49,3 prosent. (Brudd på taushetsplikt, bruk av personopplysninger uten samtykke)
- Svikt i systematisk internkontroll GDPR 6,3 prosent. (Ikke gjennomført risikovurdering, ledelsens gjennomgang ikke gjennomført, manglende opplæring av ansatte og manglende prosedyrer/retningslinjer)
- Tilgang til informasjon/system – 39,9 prosent. (For mye tilganger til personopplysninger, ikke tilstrekkelig tilgangskontroll, manglende tilgang til personopplysninger, system/teknologi ikke tilgjengelig)

I intervjuene fortelles det at det meldes mange avvik og at det er diskusjoner om hva som er avvik. Det fortelles at det er få rutiner på lukking av avvik, men at det er en felles praksis og god håndtering av avvikene. Det fortelles at det er mangelfull opplæring om avvik og en annen forteller at det er planlagt opplæring av ledere i avvikshåndtering.

3.3.11 Revisors vurdering

Revisjonskriteriet er at kommunen må ha et avvikssystem og ansatte må melde avvik.

> *Revisor vurderer at kommunen har et avvikssystem og at ansatte melder avvik, men at avvikene innenfor informasjonssikkerhet kun er knyttet til GDPR.*

Revisor finner at det meldes avvik i kommunens avvikssystem og avvikene håndteres. Avvikskategoriene er knyttet til GDPR og er ufullstendig for det mer overordnede perspektivet på informasjonssikkerhet. Revisor har ikke undersøkt om det finnes kategorier innenfor sikkerhet og beredskap som dekker informasjonssikkerhet.

3.3.12 Evaluere og lære av hendelser

Lederne skal bruke avviksstatistikk aktivt i forbedringsarbeid og i prosessen med risikovurderinger, heter det i styringsdokumentet for internkontroll i Bodø kommune. Dette for å sikre at gjentakende avvik og rullerende risikovurderinger legger grunnlag for forbedring og læring.

I oppstartsmøtet fortelles det at kommunen har en håndfull GDPR-hendelser hvert år. En av de systemansvarlige forteller at vedkommende blir involvert hvis hendelsen er knyttet til systemet vedkommende har ansvar for. En av de ansatte ved digitaliserings- og IKT-kontoret forteller at de siste årene har erfaringsutveksling blitt en del av kontorets ukentlige møter. Fra helse og omsorg fortelles det at avvikene håndteres i kvalitetssirkel slik at andre kan lære av avvikene.

GDPR-gruppen gjennomfører egenkontroller av ulike enheter i organisasjonen. Erfaringen fra dem er at egenkontrollen i seg selv bidrar til læring for de som kontrolleres. En fra GDPR-gruppen forteller at egenkontrollene handler om hvordan virksomheten jobber med GDPR og de samme spørsmålene er brukt i alle egenkontrollene. Rapportene fra egenkontrollene presenteres i ledergruppen, men vedkommende er usikker på hvordan informasjonen blir formidlet videre fra ledergruppen til de ulike avdelingene og lederne der. Vedkommende er også usikker på hvordan arbeidet GDPR-gruppen gjør blir lagt merke til hos ledelsen.

3.3.13 Revisors vurdering

Revisjonskriteriet er at kommunen bør evaluere og lære av hendelser.

Revisor vurderer at evaluering og læring av hendelser i begrenset grad er satt i system.

Revisor finner at evaluering og læring av hendelser er beskrevet i styringsdokumentet for internkontroll, men at den delen av kvalitetsarbeidet som handler om å evaluere og lære ikke gjennomføres systematisk i hele organisasjonen.

3.4 Opplæring av brukere

3.4.1 Revisjonskriterier

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

3.4.2 Opplæring

Alle ansatte skal ha opplæring i systemer som benyttes i kommunen (IKT, fagsystemer og kvalitetssystem), står det i styringsdokumentet for internkontroll i Bodø kommune. Kommunen har en sjekkliste som skal sikre nødvendig opplæring ved nyansettelser.

I Bodø kommunes sitt dokument internkontroll og informasjonssikkerhet, er en av sikkerhetsstrategiene at alle ansatte i Bodø kommune skal bli gjort kjent med og etterleve gjeldende lov- og regelverk. Dette er utdypet med at alle ansatte skal få opplæring i gjeldende interne retningslinjer, personvernlovgiving og relevante fagsystemer. E-læringssystemet (SMART-portal) kan benyttes for opplæring. Nærmeste leder skal ha en oversikt over opplæring og kompetanse hos egne medarbeidere, og har ansvaret for at egne medarbeidere får den opplæringen de har behov for. Opplæringen skal minimum omfatte:

- Retningslinjer for de ansatte i informasjonssikkerhet
- Opplæring i relevante informasjons- og fagsystem som den ansatte får tilgang til
- Relevante e-læringskurs
- Lovpålagt taushetsplikt

I dokumentet internkontroll og informasjonssikkerhet opplyses det at ansatte skal signere taushetserklæring og sikkerhetsinstruks. Under intervjuene kommer det fram at ansatte har signert taushetserklæring, men ingen kjenner til noen sikkerhetsinstruks. Det fortelles i intervjuene at det er frivillig å benytte seg av kursene som finnes i e-læringssystemet, men flere av de som har blitt ansatt den senere tiden har gjennomført e-læringskurset *Bli GDPR-superhelt*. En av de som ble intervjuet har vært med å utvikle kurset og forteller at tanken er at det skal gjennomføres hvert andre år. En annen forteller at opplæringsprogram er innkjøpt. Ansatte er ikke pålagt å gjennomføre opplæringsprogrammet, men det reklameres for det på intranett.

Informasjonssikkerhet er ikke noe tema i organisasjonen, med unntak av når det skjer en hendelse, forteller en av de ansatte. En annen forteller at det er mangel på grunnleggende dataopplæring, eksempelvis er det arbeidsprosesser hvor det brukes papir og epost i stedet for fagsystemer og sak- og arkivsystemet. I en av egenkontrollene som ble gjennomført i 2023 er det rapportert at flere har utfordringer med grunnleggende datakunnskap.

I et intervju fortelles det at GDPR-gruppen har meldt behov for utvidet kompetanse på informasjonssikkerhet. Innenfor helse har de laget huskeregler, og de har plakater for å ivareta informasjonssikkerhet.

I spørreundersøkelsen til systemansvarlige er det ni prosent som ikke har fått opplæring for å ha systemansvar. Det er 22 prosent som har fått opplæring gjennom eksterne kurs, 17 prosent gjennom interne kurs, 43 prosent i interne møter og 35 prosent individuelt av kollega. (her kunne flere alternativer velges). Kommentarene til svarene er at noen er selvlærte, andre har fått opplæring fra systemleverandør og en er usikker på om vedkommende har den kompetansen som vedkommende bør ha.

I et av intervjuene forteller vedkommende at hen har tatt initiativ til systemansvarsmøte hvert halvår, hvor alle systemansvarlige inviteres. Formålet er å øke bevisstheten og kunnskapen om rollen som systemansvarlig. I møtene deles erfaringer og kunnskap.

3.4.3 Revisors vurdering

Revisjonskriteriet er at kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Revisor vurderer at ansatte ikke får tilstrekkelig opplæring i informasjonssikkerhet.

Revisor finner at det ikke er noe tilbud om opplæring i informasjonssikkerhet til ansatte i Bodø kommune. Det er et e-læringskurs om GDPR, som er frivillig å gjennomføre. Funn viser at det er behov for grunnleggende dataopplæring og opplæring i informasjonssikkerhet.

3.5 Delkonklusjon

Problemstilling som besvares er om Bodø kommune har etablert et helhetlig styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

Revisor konkluderer med at Bodø kommune mangler et helhetlig styringssystem for informasjonssikkerhet, som tilfredsstiller krav i regelverket.

Konklusjonen er basert på at sikkerhetsstyringen i kommunen omfatter fysisk sikkerhet og personellsikkerhet og i liten grad informasjonssikkerhet. Bodø kommune har et systematisk, men ikke formalisert arbeid med GDPR, blant annet med GDPR-gruppe og flere rutiner på områder, samt at det gjennomføres egenkontroller. Dette arbeidet kan betraktes som en del av arbeidet med informasjonssikkerhet, men er løsrevet fra sikkerhetsstyringen.

Dokumentet internkontroll og informasjonssikkerhet beskriver mange sentrale forhold ved informasjonssikkerhet, utfordringen er at dokumentet ikke er implementert og etterleves ikke i praksis.

Det er gode intensjoner med å innlemme informasjonssikkerhet i internkontrollarbeidet og dette kan i beste fall sies å være underveis. Her mangler blant annet det sektorovergripende dokumentet om informasjons- og datasikkerhet, og dermed et felles grunnlag for arbeidet med internkontrollen på området.

Manglende opplæring i informasjonssikkerhet er en risiko i kommunen.

4. Tekniske og organisatoriske tiltak

Den andre problemstillingen er om kommunen har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Revisjonskriteriene er derfor ulike tekniske og organisatoriske tiltak for å ivareta informasjonssikkerheten. De er hovedsakelig hentet fra Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Grunnprinsippene er delt inn i fire kategorier, 1) identifisere og kartlegge, 2) beskytte og opprettholde, 3) oppdage og 4) håndtere og gjenopprette. Revisjonskriteriene er utledet i vedlegg to.

4.1 Identifisere og kartlegge

4.1.1 Revisjonskriterier identifisere og kartlegge

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

4.1.2 Oversikt over enheter i IKT-systemet

PCer og nettverksutstyr kjøper kommunen selv. Digitaliserings- og IKT-kontoret setter opp PCene og de innrulleres i Intune. Mobiler er ikke innrullet i Intune, men det er et ønske. Intune beskytter data, applikasjoner, identiteter og enheter til alle ansatte. Kommunen vil i løpet av året ta i bruk Autopilot, som er en automatisert løsning for idriftsetting av klienter.

Kommunen har en rutine for utskifting av PCer, men den følges ikke så godt, forteller en av de ansatte. Videre forteller vedkommende at kommunen skal bli bedre til å ha fullstendig oversikt over hvem som egentlig eier PCen og har ansvaret for den. Dette eierforholdet kommer ikke fram av dagens oversikter.

Nettbrett og mobiler på helse er innrullet i helse sin MDM-løsning (mobile device management). Det finnes nettbrett blant ansatte som Digitaliserings- og IKT-kontoret ikke forvalter. Bruken av nettbrett er ikke undersøkt nærmere.

En av de ansatte forteller at oversikten over enhetene i systemet ikke er samlet ett sted. Kommunen har verktøyene for å gjøre det, men det er en stor og vanskelig jobb.

Digitaliserings- og IKT-sjefen forteller at PCer innleveres til digitaliserings- og IKT-kontoret når ansatte slutter. Kommunen har en avtale med en ekstern aktør om resirkulering av PCer. I digitaliserings- og IKT-kontorets eget filsystem finnes det retningslinjer for avhending av PCer. Retningslinjene er stilet til medarbeidere i Bodø kommune. I forhold til sikkerhet står det at alt av innhold og programvare på PCen skal slettes på en slik måte at det ikke er mulig å gjenskape hele eller deler av innholdet i PCen. I retningslinjene står det at digitaliserings- og

IKT-kontoret skal påse at all informasjon og programvare på PCen slettes. En av de ansatte informerer om at ansatte tidligere fikk muligheten til å kjøpe utrangerte PCer, men at dette ikke er mulig lengre.

4.1.3 Revisors vurdering

Revisjonskriteriet sier at kommunen må ha en oversikt over enheter i IKT-systemet.

Revisor vurderer at kommunen har en oversikt over enheter i IKT-systemet.

Oversikten over enhetene i IKT-systemet er spredt på ulike systemer. Gjennom Intune har kommunen en god oversikt over PCer og andre enheter. Det kan være en utfordring at det finnes PCer som ikke er knyttet til en bestemt eier, eksempelvis at de brukes sjelden og utgjør en sikkerhetsrisiko hvis de ikke blir oppdatert jevnlig.

4.1.4 Oversikt over programvare

Rutinen for daglig informasjonssikkerhet sier at installasjon av programvare skal kun skje etter godkjenning av digitaliserings- og IKT-kontoret.

I Digiorden er det registret 197 programmer. I et intervju fortelles det at noen programmer ikke er registrert og i tillegg kan det være programmer som digitaliserings- og IKT-kontoret ikke kjenner til. I spørreundersøkelsen er det 96 prosent av de systemansvarlige som oppgir å ha fullført registreringen av systemet i Digiorden, mens oversikten fra Digiorden som revisor har fått tilsendt viser at registreringen ikke er fullført for mange systemer.

En av de ansatte forteller at det er vanskelig å ha en oppdatert oversikt over programvare. Ansatte kan også kjøpe nettbasert programvare, men installering blir vanskelig hvis vedkommende ikke har rettigheter. Det finnes en egen prosedyre for innføring av nye digitale systemer. Det er superadministrasjonsbruker og hjelpdesk som bistår med installering. Fjerning av programmer er opp til den enkelte avdeling å gjøre og det varierer om det blir gjort. Det er enklere å fange opp programvare som skal erstattes. Utfasing av programvare blir bedre når det flyttes ut i sky og styres gjennom Azure[5]. Da betaler kommunen for bruk, noe som betyr at det overvåkes hva som brukes.

4.1.5 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha en oversikt over programvare.

Revisor vurderer at kommunen har en nesten fullstendig oversikt over programvaren.

Gjennom Digiorden har kommunen en oversikt over programvare som kommunen bruker. Samtidig er det ansatte som kjenner til at kommunen har annen programvare som ikke er

[5] Azure er en skyplattform for blant annet infrastruktur og databehandling i skyen.

registrert der og at det ikke er noen rutine for å fjerne utdatert programvare. Ny programvare som skal installeres lokalt skal godkjennes, men det er uklart hvordan denne prosedyren håndheves. Det kan også være en sikkerhetsrisiko at programmer ikke fjernes når de er utfaset fra leverandør eller ikke er i bruk lengre.

4.1.6 Tilgangsstyring

Når en ny bruker skal få tilgang til kommunens datasystemer, skal nærmeste leder sende inn et autorisasjonsskjema til systemansvarlig der aktuelle tilgangsnivåer for den nye brukeren er spesifisert. Når ansettelsesforholdet avsluttes, er det nærmeste leder sitt ansvar å sørge for at brukeren slettes. Dette framgår av dokumentet internkontroll og informasjonssikkerhet. Videre er det presisert at alle virksomheter skal til enhver tid følge gjeldende rutiner for tilgangsrettigheter til de aktuelle fagsystemene.

Dokumentet internkontroll og informasjonssikkerhet har to sikkerhetsstrategier om tilgangsstyring.

- Personer i Bodø kommune skal gis tilgang i henhold til fastsatte prinsipper for tilgangsstyring.
- Gjennom sikker identifisering sikre at personopplysninger kun blir tilgjengelig for rett person.

I intervjuene fortelles det at kommunen bruker AD (active directory). Kommunen har programvare med livsløpshåndtering av ansattekontoer som er koblet mot personalsystemet. Ikke alle brukerkontoer i AD er generert av programvaren for livløpshåndtering, noe som innebærer at tilgangen ikke styres fra AD. Det er den enkelte leder som har ansvar for systemer som ligger utenfor AD. En av de som ble intervjuet fortalte om en svakhet i systemet, som digitaliserings- og IKT-kontoret ikke har prioritert å rette.

En ansatt forteller at vedkommende rydder i tilganger en gang per halvår, men vurderer å gjøre det hyppigere. En annen har ingen fast rutine for å rydde i tilganger, men gjør det når vedkommende har mulighet. I spørreundersøkelsen svarer 65 prosent av de systemansvarlige at de både må gi og fjerne tilganger til systemene, mens tilgangene styres gjennom AD for 22 prosent av de systemansvarlige. En opplyser i tillegg at det finnes flere superbrukere som tildeler tilganger. En annen opplyser at noen tilganger gis av driftsleverandør, men godkjennes av vedkommende som er systemansvarlig.

Spørreundersøkelsen viser at blant de som fjerner tilganger, gjør 27 prosent det en gang per måned eller oftere, 27 prosent en gang per kvartal, 33 prosent en gang per halvår og 13 prosent årlig eller sjeldnere.

En av de ansatte forteller at ved nyansettelser skjer det en totalgjennomgang om hvilke tilganger som trengs. Tilganger vurderes ut fra tjenstlige behov. Det er avdelingsdirektøren som beslutter. Brukerne oppretter selv passord etter å ha identifisert seg med bankID. Det

finnes regler for passordbytte, men disse kjenner vedkommende ikke til. Det fortelles at kommunen har en pilot på tofaktor autentisering samt at det kommer krav om multifaktor autentisering. Det er krav om passordkompleksitet. Kravene til passord finnes på www.samkos.no[6]. På samkos.no finnes også prosedyre for bestilling av tilganger og der finnes et skjema som må fylles ut. Digitaliserings- og IKT-sjefen forteller at ingen rettigheter tildeles uten at disse skjemaene er utfylt og godkjent av autorisert personell.

En annen forteller at det mangler prosedyrer for hvem som skal godkjenne endringer i tilganger. Det fortelles også at kommunen har mange eksterne og midlertidige brukere, og vedkommende mener det ligger for mange eksterne brukere i systemet. En annen forteller at kommunen ligger over måltall for eksterne brukere med tilgang. Eksterne med tilgang må signere taushetserklæring og de registreres i personalsystemet. (Revisor har ikke undersøkt om eksterne har signert taushetserklæring)

I spørreundersøkelsen svarer 78 prosent at det er eksterne (ikke ansatt i Bodø kommune) som har tilganger i systemet vedkommende har ansvar for.

4.1.7 Revisors vurdering

Revisjonskriteriet sier at kommunen må ha et system for styring av tilganger.

> *Revisor vurderer at kommunen har et system for styring av tilganger, men at systemet ikke dekker tilganger til alle systemer.*

Kommunens system for tilgangsstyring er koblet til personalsystemet og et aktivt arbeidsforhold. Det er den enkelte leder som gjøre en behovsvurdering av hvilke tilganger den enkelte har behov for. Ikke alle tilganger til programvare styres gjennom dette systemet, noe som betyr at tilganger også må gis og avvikles manuelt. Utfordringen er å avvikle tilganger, og systemansvarlige må rydde i tilganger på de systemene som ikke styres via personalsystemet. Revisor ser at det kan være utfordringer med at mange eksterne har tilganger til ulike systemer og spesielt i forhold til nivået på tilganger.

Den enkeltes tilgang til systemene krever identifisering med bankID ved oppstart. Dette er et sikkerhetstiltak. Det er en svakhet at flerfaktorautentisering ikke er tatt i bruk, samt varierende oppfølging av tilganger som allerede er gitt.

4.2 Beskytte og opprettholde

4.2.1 Revisjonskriterier beskytte og opprettholde

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.

[6] Samkos – samhandlende kommuner i Salten. Dette er et nettsted for hjelp og støtte innenfor IKT, en portal til støttefunksjoner og tjenester tilgjengelig for Bodø kommune og andre samarbeidende kommer.

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

4.2.2 Anskaffelses- og utviklingsprosesser

I oppstartsmøtet fortelles det at ved anskaffelser av nye IT-løsninger har kommunen blitt mer bevisst på å ta hensyn til informasjonssikkerhet.

I kommunens dokument internkontroll og informasjonssikkerhet er en av sikkerhetsstrategiene at det skal tas hensyn til personvern i alle utviklingsfaser ved større endringer eller anskaffelser av nye informasjonssystem (innebygd personvern).

I dag finnes det ingen rutiner for å melde behov, endret behov eller rutiner for å gjøre innkjøp, forteller en av de ansatte. Vedkommende holder på å utarbeide en veileder for innføring av nye digitale systemer, utformet som et flytskjema. Ifølge flytskjemaet har digitaliserings- og IKT-kontoret en rolle i den første fasen, som er behovsinnmelding. I fasen før innføring skal det kartlegges behov for integrasjoner og eventuelle virksomhetssertifikat. I tillegg skal det defineres nødvendige krav til IKT, nettverk og datasikkerhet, og det skal lages et støttedokument som inneholder disse kravene.

Det fortelles av digitaliserings- og IKT-kontoret ønsker å være påkoblet tidlig i anskaffelses-prosessen, men ofte skjer det ikke før helt på slutten. Digitaliserings- og IKT-kontorets rolle er å få bekreftelse på at programmet skal ligge i Digiorden med riktig informasjon.

I et intervju fortelles det at digitaliserings- og IKT-kontoret har instruert innkjøpskontoret om at digitaliserings- og IKT-kontoret skal uttale seg om tilgangsstyring før anskaffelse. Arkiv må også med i disse prosessene, spesielt når det er arkivverdig informasjon i systemet som skal anskaffes. Fra helse- og omsorgsavdelingen fortelles det at norm for informasjonssikkerhet[7] brukes ved anskaffelse av systemer. I dette arbeidet ivaretas sikkerhetsperspektivet av tilgjengelig kompetanse hos de som har ansvar for prosesser rundt anskaffelse av nye systemer.

I månedsrapporten for april fra driftsleverandøren opplyses det at det er en stor risiko for Bodø kommune at så mange prosjekter som medfører endringer i produksjonen pågår samtidig. Det er i tillegg omtalt at flere av de kritiske og alvorlige hendelsene som rapporteres ble forårsaket av endringer som ble gjort av driftsleverandøren, men i regi av et prosjekt i kommunen som hadde ansvaret for endringen.

[7] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren er en etablert bransjenorm som stiller en rekke krav til, og veileder om, hvordan informasjonssikkerhet og personvern skal ivaretas i helse- og omsorgssektoren. (www.helsedirektoratet.no/tema/kunstig-intelligens/personvern- og-informasjonssikkerhet)

4.2.3 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.

Revisor vurderer at sikkerheten ikke ivaretas i anskaffelses- og utviklingsprosesser.

Det finnes eksempler på at sikkerheten ivaretas i anskaffelses- og utviklingsprosesser, men dette er ikke satt i system. Digitaliserings- og IKT-kontoret opplever at de kommer sent inn i anskaffelsesprosesser og det samme gjelder arkiv. Digitaliserings- og IKT-kontoret har utarbeidet forslag til en prosedyre for gjennomføring av anskaffelser. Revisor finner at ansatte som arbeider med utviklingsprosesser i kommunen har oppmerksomhet på sikkerhet i utviklingsprosesser i kommunen.

4.2.4 Ansvar for sikkerheten ved tjenesteutsetting

Bodø kommune kjøper driftstjenester fra en leverandør. Kommunen har hatt ekstern driftsleverandør siden 2004. Den forrige avtalen var en totalpakke, mens dagens avtale er en ren driftsavtale. Det som mangler i dagens driftsavtale er utstyrsavtale, WAN[8] avtale, telefoniavtale, utviklingsavtale og sikkerhetsavtale, forteller en av de ansatte.

De tekniske kravene i konkurransegrunnlaget er det kommunen som har stilt og et konsulentselskap bisto kommunen som rådgiver. Tre ansatte ved digitaliserings- og IKT-kontoret deltok i anskaffelsen. I tillegg ble brukere fra Bodø kommune involvert i konkrete spørsmål knyttet til tjenesten eller systemet. Det ble også brukt juridiske ressurser for å sikre at utformingen av konkurransen var i samsvar med regelverket.

I driftsavtalen er de tre fra digitaliserings- og IKT-kontoret oppgitt som autorisert personale i forbindelse med administrasjon og oppfølging av driftstjenestene. I tillegg er det fire andre ansatte ved digitaliserings- og IKT-kontoret som kan være aktuelle innenfor spesifikke områder.

I kravspesifikasjonen til driftsavtalen er det satt noen overordnede føringer for å ivareta informasjonssikkerheten.

- Leverandøren må levere overvåking og drift av sikkerhetsløsninger og ha et høyt beredskaps- og kompetansenivå knyttet til dette.
- Det skal settes høye krav når det gjelder sikkerhet mot uautorisert tilgang til data, oppetid og mulig tap av data.
- Det skal gjennomføres løpende sårbarhetsanalyser og iverksettelse av nødvendige tiltak for å eliminere den risiko som avdekkes.
- Det skal etableres plan for tiltak ved alvorlige feil samt rekonstruksjon av data.

[8] WAN (wide network area) er et datanettverk for et større geografisk område-

Videre står det i kravspesifikasjonen at driftsløsning skal sikre mot alle typer virusangrep og spam, samt filtrering av uønsket innhold. Dette gjelder også innbrudd på klienter og servere. I tillegg er det listet opp 12 generelle krav. Et av dem er at informasjonssikkerheten skal være i tråd med ISO 27001 og ISO 27002 eller tilsvarende.

I leverandørens svar på utlysningen oppgis det at sikkerhetstjenester for leveransen omfatter (forkortet versjon):

- Sikkerhetsleder (Security Manager)
- Sårbarhetsscan og håndtering – tjeneste for kontinuerlig scanning av kundens infrastruktur (datasenter) for å identifisere og håndtere sårbarheter og rådgiving av sårbarhetsekspert.
- Endepunktssikkerhet – 24/7 overvåkning og respons fra leverandørens SOC-tjeneste[9].
- Penetrasjonstesting – på årlig basis av kundefront.
- Brannmur
- Epostbeskyttelse

En av de ansatte forteller at det varierer hvordan driftsleverandøren ser på sikkerhet og er usikker på grenseflata mellom kommunen og driftsleverandøren. Forventningsavklaringene er ikke optimale. Avtalen er omfattende og all informasjonen i avtalen er ikke delt med alle på digitaliserings- og IKT-kontoret og da kommer den ikke ut i organisasjonen heller. Vedkommende mener at for mye er outsourcet til driftsleverandøren og er ikke fornøyd med avtaleteksten og hvordan driftsleverandøren etterlever den.

4.2.5 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.

> *Revisor vurderer at ansvarsfordelingen mellom kommunen og driftsleverandøren er noe uklar når det gjelder sikkerheten.*

Vurderingen bygger på at det er få ved digitaliserings- og IKT-kontoret som har innsikt i driftsavtalen og ulike forhold som berører informasjonssikkerhet der. Driftsavtalen ivaretar datasikkerhet og i mindre grad informasjonssikkerhet. Når kommunen ikke har et helhetlig styringssystem for informasjonssikkerhet, mangler rammeverket for hvilke krav som skal stilles til datasikkerhet i driftsavtalen.

Områdene datasikkerhet og informasjonssikkerhet er i stadig utvikling, og det er krevende for kommunen å følge opp denne utvikling. I den sammenheng er det betryggende å ha en driftsleverandør. På den annen side er det krevende for kommunen å ha tilstrekkelig bestillerkompetanse for å klare å bestille den driftstjenesten som kommunen har bruk for. I

[9] SOC – Security operation center.

dette arbeidet har kommunen benyttet seg av konsulenter, noe som er bra. Samtidig har konsulenter begrenset kjennskap til kommunens behov.

Når det i kravspesifikasjonen står at driftsløsning skal sikre mot alle typer virusangrep og spam samt filtrering av uønsket innhold, vitner det om urealistiske krav. Trusselbildet er i stadig utvikling og det er vanskelig å sikre kommunen mot alle typer angrep. Samtidig er det slik at kommunens ansatte, som har mangelfull opplæring (jfr. 3.4) utgjør en risiko når det kommer til å trykke på lenker eller utsettes for andre uønskede hendelser. Det at kommunen ikke har tatt i bruk flerfakturautentisering øker også risikoen. Opplæring og flerfaktorautentisering er to elementer i et helhetlig styringssystem hvor svakheter med dem ikke kan dekkes opp av en driftsavtale.

4.2.6 Sikker IKT-struktur

I dokumentet internkontroll og informasjonssikkerhet er en av sikkerhetsstrategiene at informasjonssystemet i Bodø kommune skal konfigureres og forvaltes slik at tilfredsstillende informasjonssikkerhet oppnås. En annen sikkerhetsstrategi er at opplysningene skal behandles i tråd med reglene om taushetsplikt og være beskyttet, slik at uvedkommende ikke får kjennskap til dem.

I ROS 2018 for Bodø kommune er at av tiltakene ved bortfall av infrastruktur at det skal utarbeides en konfigurasjonsoversikt over hvordan IKT-systemene i kommunen holder sammen.

Nettverket er segmentert, forteller en av de ansatte. Det er fildeling mellom sikker og vanlig sone, noe vedkommende ønsker å stenge for. Vedkommende håper at driftsleverandøren har kart over kommunens nettverk. Nettverket er komplekst og når mer utstyr og enheter tas i bruk, krever det utvidelse av kapasiteten. I tillegg er det behov for å skille tydeligere mellom utstyr som er sensitivt og utstyr som er mindre sikkert. Det at kommunen har flyttet mye av tjenestene ut i sky, gjør systemet mer komplekst når ulike deler skal snakke sammen på tvers av alle disse datasentrene.

En av de ansatte forteller at de har gjort en jobb for å dokumentere status på sikkerhet og identifisere forbedringer, ved hjelp av en aktuell programvare som samler relevant data fra IT-miljøet. Sluttresultatet er en risiko- og faktabasert handlingsplan for å forbedre organisasjonens sikkerhet, og kommunen scoret middels på denne gjennomgangen.

Digitaliserings- og IKT-kontoret er flinke til å tenke sikkerhet, men det er mange av de systemansvarlige ute i organisasjonen som ikke har med seg det perspektivet. Spørsmål rundt sikkerhet er mer komplekst og sammensatt enn bare for noen år siden, forteller en av de som ble intervjuet.

I driftsavtalen finnes en overordnet beskrivelse av sikkerhetsarkitekturen. I de administrative bestemmelsene skal det være jevnlige møter (hver måned eller 14. dag) mellom kommunen og driftsleverandøren med diskusjoner om arkitektur, design og endringer i driftsløsningen.

4.2.7 Revisors vurdering

Revisjonskriteriet sier at kommunen bør etablere og dokumentere en sikker IKT-arkitektur.

> *Revisor vurderer at kommunen har bestilt en sikker IKT-arkitektur fra driftsleverandøren og at driftsleverandørens beskrivelse av IKT-arkitekturen inneholder relevante sikkerhetsmekanismer.*

Driftsleverandøren har en beskrivelse av IKT-infrastrukturen, men revisor har ikke undersøkt nærmere om den er slik den er beskrevet. Dette har ikke revisor kompetanse til, men fra intervjuene kommer det fram noen svakheter med systemet slik det er satt opp. Dette gjelder at det er mulig med fildeling mellom sikker og vanlig sone samt, at det er behov for tydeligere skiller mellom utstyr som er mer sensitivt enn ordinært. Økt bruk av skybaserte løsninger er et sikkerhetstiltak, men det gjør systemet mer komplekst.

4.2.8 Sentral styring med sikkerhetsoppdateringer

I oppstartsmøtet fortelles det at avdelingsdirektørene er systemeier, og har det formelle ansvaret med å ivareta sikkerhet for systemene de eier. Etterlevelsen i praksis er best på helse og omsorg.

På systemer som digitaliserings- og IKT-kontoret har ansvar for kjøres det sikkerhets-oppdateringer til faste tidspunkt hver uke. Hvis det er kritiske oppdateringer gjennomføres de uavhengig av det faste tidspunktet. Brukerne har begrensede muligheter til å hoppe over sikkerhetsoppdateringer før de installeres. Det skal ikke forekomme at PCer ikke blir oppdatert, men det kan skje ute på enhetene med PCer som ikke er koblet til nettet.

Når systemansvaret ligger ute på enhetene har ikke digitaliserings- og IKT-kontoret kontroll på oppdateringer. En av de ansatte mener at systemansvaret burde vært sentralisert fordi det er stor variasjon i hvordan systemansvaret ivaretas.

I gjennomføringen av spørreundersøkelsen er det identifisert at 39 personer har systemansvar i Bodø kommune og flere av dem har ansvar for flere systemer. Det er 57 prosent av de systemansvarlige som har en bestemt ansatt som ivaretar systemansvaret hvis vedkommende er fraværende over litt tid. Det er 17 prosent som oppgir at de har en egen rutine for sikkerhetsoppdateringer, mens 48 prosent følger en felles rutine og 35 prosent oppgir at det ikke finnes noen rutine.

Noen programmer oppdaterer seg selv, forteller en av de ansatte. Det finnes programmer som ingen har et definert ansvar for og da blir oppdateringer tilfeldig.

Revisor har mottatt to rapporter over patcher[10] som er gjennomført i april 2024. Disse gjennomgås i månedlig driftsmøte med driftsleverandøren. Den månedlige driftsrapporten fra driftsleverandøren viser at det ble patchet 60 servere og av disse måtte fire servere patches manuelt. Videre ble det gjort 124 patcher i sky.

4.2.9 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha sentral styring med sikkerhetsoppdateringer.

Revisor vurderer at kommunen ikke har sentral styring med sikkerhetsoppdateringer.

Vurderingen er basert på at sikkerhetsoppdateringer er spredt rundt i organisasjonen. Digitaliserings- og IKT-kontoret gjør jevnlige sikkerhetsoppdateringer på de systemene de har ansvar for. Programvare som ligger i sky oppdateres automatisk, men svakheten er fagprogrammer som finnes lokalt i organisasjonen. Spørreundersøkelsen viser at alle ikke har rutiner for sikkerhetsoppdateringer. I tillegg hevdes det at det finnes programvare i organisasjonen som digitaliserings- og IKT-kontoret ikke har oversikt over (jf. 4.1.4).

4.2.10 Plan for sikkerhetskopiering og ta sikkerhetskopier

I kundens kravspesifikasjon til driftsavtalen står det at leverandøren skal etablere en plan for utførelse av sikkerhetskopi (backup) og at kunden skal godkjenne denne planen. Dette har leverandøren svart ja på i tilbudet. Revisor har etterspurt om denne planen finnes, men har ikke fått noen bekreftelse på det.

Ifølge driftsavtalen skal full sikkerhetskopi av databaser beholdes hver dag siste 7 dager. Det skal også beholdes en versjon som er henholdsvis 14 dager, en måned og tre måneder gammel. Ved sletting av databaser skal det tas full backup og den skal beholdes i 180 dager. I den månedlige driftsrapporten er det i tillegg rapportert at databaser skal kunne tilbakestilles til point-in-time i serviceperiode B, siste to dager.

En av de ansatte forteller at driftsleverandøren tar sikkerhetskopi og kommunen får rapporter. Kommunen kjenner til hvor dataene lagres. En annen forteller at det er en risiko hvis sikkerhetskopien ikke er sikret på en sikker måte.

I den månedlige driftsrapporten fra driftsleverandøren opplyses det at det brukes tre ulike systemer for sikkerhetskopiering i Bodø kommune og linkene til rapportene fra de tre systemene ligger i rapporten.

Revisor har mottatt to rapporter fra sikkerhetskopiering gjennomført av driftsleverandøren. Begge rapportene viser at sikkerhetskopiering er gjennomført. Rapportene er for april og den ene er generert 13.05.2024 og det angis hvor lenge sikkerhetskopien lagres. Den ene

[10] En patch er en spesifikk reparasjon av et problem eller en sårbarhet, mens en oppdatering er mer omfattende og inneholder ulike endringer og forbedringer. (www.ninjaine.com/blog/patch-vs-update)

sikkerhetskopien omfatter det som ligger i sky mens den andre omfatter data som er lagret lokalt i kommunen.

I driftsleverandørens tilbud er sikring av sikkerhetskopier beskrevet. Data som lagres i driftsleverandørens private sky (et av tre systemer for sikkerhetskopiering) er basert på immutable architecture, som betyr at data ikke kan overskrives. Den delen av driftsavtalen som beskriver tjenestenivået sier ikke noe om ikke-overskrivbar sikkerhetskopiering.

4.2.11 Revisors vurdering

Revisjonskriteriet sier at kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

> *Revisor vurderer at kommunen ikke kjenner til planen for sikkerhetskopiering, men kommunen får månedlige driftsrapporter med informasjon om sikkerhetskopiering.*

Driftsleverandøren har ansvaret for sikkerhetskopiering og det er få av de ansatte i kommunen som kjenner til hvordan dette skjer, med unntak av det som rapporteres. Ifølge driftsavtalen skal leverandøren utarbeide en plan for sikkerhetskopiering som kommunen skal godkjenne. Revisor har etterspurt planen, men ikke fått noen bekreftelse fra kommunen på at planen finnes.

4.3 Oppdage sårbarheter, trusler og hendelser

4.3.1 Revisjonskriterier oppdage

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

4.3.2 Hva skal sikkerhetsovervåkes

I dokumentet internkontroll og informasjonssikkerhet, er det to sikkerhetsstrategier som handler om sikkerhetsrelevante data.

- Alle tilganger skal registreres i form av logger i helseregistre (inkludert elektronisk pasientjournal)
- For å sikre sporbarhet skal det registreres i behandlingen hvem som har foretatt registrering, endring, retting og sletting.

I kommunens kravspesifikasjon til driftsavtalen er det stilt krav til informasjonssikkerhet og sikkerhetsløsninger. De overordnede føringene er:

- … overvåkning og drift av sikkerhetsløsninger og ha at høyt beredskaps- og kompetansenivå knyttet til dette.
- … høye krav når det gjelder sikkerhet mot uautorisert tilgang til data, oppetid og mulig tap av data.
- .. gjennomføres løpende sårbarhetsanalyser og iverksettelse av nødvendige tiltak for å eliminere den risiko som avdekkes.
- … etablere en plan for tiltak ved alvorlige feil samt rekonstruksjon av data.

Videre står det at driftsløsningen skal sikre mot alle typer virusangrep og spam, samt filtrering av uønsket innhold.

I driftsavtalen står det at gjennom etableringsprosjektet skal det avtales i detalj hva som skal overvåkes, logges og i hvilke situasjoner kommunen skal varsles, eksempelvis nettverkskomponenter og kommunikasjonslinjer, avtalte applikasjoner og gjennomføring av sikkerhetskopiering og automatiserte jobber. Revisor har etterspurt dokumentasjon på disse avklaringene som skulle vært gjort i etableringsprosjektet, men har ikke fått klarhet i om det finnes.

I de administrative bestemmelsene til driftsavtalen står det at driftsleverandøren skal overvåke tjenestene og leveranseprosessene blant annet med hensyn til:

- Tilgjengelighet og responstider
- Kundens lokale infrastruktur
- Prosesser, prosedyrer og rutiner
- Sikkerhet (drift og informasjon)

4.3.3 Revisors vurdering

Revisjonskriteriet sier at kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.

> *Revisor vurderer at kommunen har lite spesifikke krav til hvilke deler av IKT-systemet som skal overvåkes.*

Kravspesifikasjonen til driftsavtalen gir overordnede krav til hva som skal overvåkes. Slik revisor forstår kravspesifikasjonen og driftsavtalen er det opp til driftsleverandøren å sikre en overvåkning og drift av sikkerhetsløsninger og ha et høyt beredskaps- og sikkerhetsnivå knyttet til dette. Det er lagt lite føringer fra kommunens side om hva som anses som kritiske deler av IKT-systemet og som trenger overvåkning. Dette kan igjen ha sammenheng med at det er mangelfullt med risikovurderinger innenfor informasjonssikkerhet (jr. kapittel 3.4.4 og 3.4.5).

4.3.4 System for å overvåke sikkerheten

I kommunens kravspesifikasjon til driftsavtalen står det at leverandøren må levere overvåkning og drift av sikkerhetsløsninger og ha et høyt beredskaps- og kompetansenivå knyttet til dette. Dette løses av kunden med kontinuerlig scanning av kundens infrastruktur for å identifisere og håndtere sårbarheter, endepunktbeskyttelse med 24/7 overvåkning og respons fra driftsleverandørens SOC-tjeneste[11]. Videre inngår årlige penetrasjonstester, kontroll av trafikk i brannmurer og epostbeskyttelse.

Kommunen overvåker lite selv, men de har en enkel SOC-tjeneste, forteller en av de ansatte. Driftsleverandøren gjør tilsvarende analyser med andre verktøy og kommunen blir varslet ved alvorlige feil. I driftsrapporten for april 2024 er det rapportert fire hendelser om mulig ondsinnet programvare og et tilfelle av å ha trykket på lenke og eposter er gått ut. Den ansatte ønsker at digitaliserings- og IKT-kontoret skal ta et større ansvar for overvåkningen og ikke overlate alt til eksterne.

I driftsavtalen står det at leverandøren har ansvaret for overvåkning av tjenestene og skal rapportere til kommunen om avvik eller hendelser som indikerer at hele eller deler av tjenestene er utilgjengelig eller står i fare for å bli utilgjengelig.

Driftsleverandørens tilbud omfatter overvåkning som omfatter prosesser i applikasjonens plattform som applikasjonen er avhengig av for å fungere, integrasjoner som det er mulig å overvåke med standard overvåkningsverktøy samt forhåndsdefinerte innslag i logger beskrevet av applikasjonsleverandøren som er mulig å overvåke med standard overvåkningsverktøy. I tillegg er det beskrevet ytelsesovervåkning på nettverk og overvåkning av nettverksenheter hos kommunen.

Kommunen benytter SIEM[12] for administrasjon av sikkerhetsinformasjon og -hendelser, forteller en av de ansatte. Det finnes mange logger, men det er ingen aktiv overvåkning og ingen har ansvar for å følge opp. Vedkommende er usikker på hva driftsleverandøren gjør. Hvis det kommer en henvendelse, er det mulig å undersøke loggene. Loggene oppbevares lenge og kommunen har mulighet til å gå tilbake å lete i dem. Pålogging på Office blir logget og det kommer varsel ved mistenkelig aktivitet. Vedkommende er usikker på om det er logger på sak- og arkivsystemet.

I tillegg til egen overvåkning mottar kommunen varsel fra KommuneCert og HelseCert på trusler og sårbarheter som oppstår.

[12] SIEM – Security information and event management.

4.3.5 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.

> *Revisor vurderer at både kommunen og driftsleverandøren har system for å overvåke sikkerheten, mens det er driftsleverandøren som analyserer data fra overvåkningen.*

I et overvåkningssystem kan det genereres mange logger og sikkerhetsdata. Utfordringene er å analysere loggene, fordi dette er tidkrevende. Både kommunen og driftsleverandøren har overvåkning i form av logger. Informasjon fra intervjuene tyder på at det er lite kjent i organisasjonen hva som overvåkes og at dette i stor grad er overlatt til driftsleverandøren.

4.4 Håndtere og gjenopprette

4.4.1 Revisjonskriterier håndtere og gjenopprette

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

4.4.2 Plan for hendelseshåndtering

I dokumentet internkontroll og informasjonssikkerhet står det at større sikkerhetshendelser skal håndteres i henhold til Bodø kommune sin overordnede beredskapsplan. Leder av kriseledelsen har myndighet til å samle nødvendig kompetanse og ressurser til å håndtere hendelsen.

Følgende beredskapstiltak ligger i beredskapsplanen tilhørende ROS-analysen fra 2018:

- Etablere manuelle rutiner for utføring av viktige oppgaver dersom tele og IT faller bort.
- Nødstrøm.
- Databehandleravtaler.
- Bygge redundante løsninger for drift av kritiske tjenester.
- Utarbeide konfigurasjonsoversikt.
- Utarbeide beredskapsplan IKT.
- Utarbeide ROS-analyse IKT.

I et av intervjuene fortelles det at plan for håndtering og gjenopprettelse er det andre som har kontroll på og inngår som en del av driftsavtalen. En annen forteller at i driftsavtalen er det ikke garanterte at kommunen får hjelp ved en uønsket hendelse.

I kravspesifikasjonen til driftsavtalen står det at driftsleverandøren skal utføre nettverksovervåkning og sørge for at sikkerhetshendelser blir stoppet og at kommunen blir

varslet. Driftsleverandøren tilbyr Incident Management Process som en integrert del av driftsleverandørens daglige drift. Sikkerhetshendelser håndteres i henhold til denne prosessen og er integrert med kommunens Incident Management Process. Driftsleverandøren tilbyr også ressurser gjennom Emergency Incident Response funksjon (CSIRT/ CIRT).

I tilbudet fra driftsleverandøren inngår det en definert informasjonsprosess i tilfelle det oppstår en kritisk sikkerhetshendelse. Videre utføres en diagnose og det iverksettes en eventuell undersøkelse.

I oppstartsmøtet informeres det om at kommunen årlig melder omkring fem saker til Datatilsynet, men har ikke hatt større hendelser. Hendelsene som er meldt har vært menneskelig glipp, for eksempel publisering av navn og personnummer på kommunens hjemmeside.

I intervjuene henviser flere til kommunens krisehåndteringsplan og tiltakskort i krisehåndteringsverktøyet. En har hørt om handlingsplanen, men ikke sett den. Videre forteller vedkommende at den skal være utskrevet og skal finnes et sted. En annen forteller at det ikke finnes noen helhetlig plan og at hendelseshåndteringen varierer etter hvilket system som blir berørt. Vedkommende forteller at det er vanskelig å lage en plan eller oversikt over hva som kan skje ettersom verdikjedene er blitt kompleks. Små hendelser kan ramme kommunen til dels hardt.

Den enkelte tjeneste skal ha oversikt over brukere, kontaktinformasjon, medisiner og tiltaksplan på papir, fortelles det fra helse. Det vil variere hvor lenge enhetene klarer seg. Det er eksempelvis mulig å skrive journal, men historikken er ikke tilgjengelig. På helse finnes det plan B-prosedyrer hvis teknologien faller bort.

4.4.3 Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha en plan for hendelseshåndtering.

Revisor vurderer at kommunen ikke har en egen plan for hendelseshåndtering.

I kommunens beredskapsplan er et av tiltakene å utarbeide en beredskapsplan IKT. Revisor har ikke funnet en slik plan. Driftsavtalen beskriver håndtering av ulike hendelser, men flere av disse er hendelser knyttet til daglig drift og ikke kritiske hendelser. Nasjonal sikkerhetsmyndighets sitt grunnprinsipp om en hendelseshåndteringsplan handler om å ha et planverk for å ivareta behovet for virksomhetskontinuitet ved beredskap og kriser. Revisor oppfatter at hendelseshåndteringen i driftsavtalen i liten grad dekker det behovet kommunen har hvis det skjer en krise på informasjonssikkerhet slik at datasystemet er mer eller mindre utilgjengelig over flere dager. En IKT-hendelse trenger ikke bare å berøre kommunens informasjonssystem, men vil ofte ha andre følgehendelser som ligger utenfor driftsleverandørens ansvar.

4.4.4 Plan for gjenoppretting

Kommunens kravspesifikasjon inneholder krav til tilgjengelighet av sine IKT-løsninger og leverandøren skal bidra til å ivareta fortsatt sikker drift av driftsleverandørens tjenester i tilfelle en krisesituasjon skal inntreffe. Driftsleverandøren skal utarbeide en beredskaps- og katastrofeplan for tjenesten. Driftsleverandøren skal her spesifisere hvilke områder vedkommende kan ta ansvar for i en krisesituasjon og hva kunden selv må ta ansvar for. Revisor har etterspurt om denne planen finnes, men har ikke fått det bekreftet.

Driftsleverandørens tilbud har tilleggstjenester for gjenoppretting av sikkerhetskopierte data i oppbevaringsperioden. Recovery Point Objetive er 24 timer ettersom sikkerhetskopier tas daglig. Målet for Recovery Time Objektive er 100 GB per time.

Driftsleverandøren anbefaler i sitt tilbud tiltak for katastrofegjenoppretting, gjennom at kommunen bygger en DR-plan for gjenoppretting i DR Scenario. Revisor har ikke undersøkt nærmere om dette er gjort.

Driftsleverandøren har tilbydd en tilleggstjeneste med ikke-overskrivbar lagring av data, slik det er for data som lagres i driftsleverandørens datasenter. Driftsavtalens del om tjenestenivået har ingen bestemmelser om ikke-overskrivbare data. Denne delen av driftsavtalen har en bestemmelse om tilbakestilling etter krisesituasjon.

> *Etter en eventuell krisesituasjon skal løsningen innen 24 timer (beregnet fra krisetidspunktet) ha minimum 50 prosent av den kapasitet som produksjonsmiljøet hadde rett forut for krisetidspunktet, samt ha full funksjonalitet og inneholde alle applikasjonsdata (inkludert arkivdata). … innen 48 timer beregnet fra krisetidspunktet) ha 100 prosent av den kapasitet som produksjonsmiljøet hadde rett forut for krisetidspunktet, samt ha full funksjonalitet og inneholde alle applikasjonsdata (inkludert arkivdata).*

I intervjuene fortelles det at det er ulike framgangsmåter for gjenoppretting og ulike scenario for feil. Digiorden gir en viss oversikt over hvor ting ligger, men kommunen er avhengig av hjelp av avtalepartene.

4.4.5 Revisors vurdering

Revisjonskriteriet sier at kommunen må ha en plan for gjenoppretting.

> *Revisor vurderer at kommunen har elementer av en plan for gjenoppretting i driftsavtalen.*

I driftsavtalen beskrives avtalte rammer for gjenoppretting ved en krise. Kravene om tilbakestilling etter en krise, slik de er beskrevet i driftsavtalen, virker urealistiske med referanse til de utfordringene som eksempelvis Østre-Toten kommune hadde etter at deres datasystem ble angrepet. I dette bildet må det også tas med i betraktningen at metoder for å

kompromittere datasystemer er i stadig utvikling, slik at en kommune ikke alltid kan forutse hva den skal beskytte seg mot.

4.5 Delkonklusjon

Problemstillingen som besvares er om Bodø kommune har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten.

> *Revisor konkluderer med at Bodø kommune ikke har tilfredsstillende organisatoriske og tekniske tiltak på plass for å ivareta informasjonssikkerheten.*

Når det mangler et helhetlig styringssystem for informasjonssikkerhet, mangler rammeverket for hvilke tekniske og organisatoriske tiltak som må på plass for å ivareta den informasjonssikkerheten som kommunen ønsker å ha. Driftsavtalen som Bodø kommune har, ivaretar viktige områder på datasikkerhet, mens tekniske og organisatoriske tiltak på andre områder innenfor informasjonssikkerhet har liten oppmerksomhet eller er fraværende.

Når Bodø kommune kjøper tjenester til drift av IKT krever det god bestillerkompetanse for å spesifisere hva de har behov for, samt for å følge opp driftsavtalen på et område som er i stadig utvikling. Når driftstjenestene kjøpes, kan det oppstå uavklarte forhold i grenseflaten mellom kommunen og driftsleverandøren.

En svakhet er at kommunen har overlatt mye til driftsleverandøren og har liten bevissthet omkring hva kommunen har behov for. Det å ha en ekstern driftsleverandør gjør at kommunen benytter seg av ekspertise på området, som har større muligheter for å følge med på utvikling innenfor spesielt datasikkerhet, sammenlignet med hva de fleste kommuner har ressurser til. Det er flere av de organisatoriske tiltakene som kommunen er den nærmeste til å håndtere, eksempelvis tilgangsstyring, anskaffelses- og utviklingsprosesser, krav til sikkerhetsoppdateringer, sikker infrastruktur, plan for hendelseshåndtering og plan for gjenoppretting.

5. Oppsummering og konklusjon

Den første problemstillingen som besvares er om Bodø kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

> *Revisor konkluderer med at Bodø kommune ikke har etablert et helhetlig styringssystem for informasjonssikkerhet, som tilfredsstiller krav i regelverket.*

Den andre problemstillingen som besvares er om Bodø kommune har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten.

> *Revisor konkluderer med at Bodø kommune ikke har tilfredsstillende organisatoriske og tekniske tiltak på plass for å ivareta informasjonssikkerheten.*

6. Anbefalinger

Revisor anbefaler kommunedirektøren å vurdere følgende:

- Etablere et helhetlig styringssystem for informasjonssikkerhet.
- Sørge for å komplettere registrering av behandlingsprotokoller, herunder ferdigstille DPIA og databehandleravtaler.
- Gi ansatte opplæring i informasjonssikkerhet.
- Gjennomgå driftsavtalen og følge den opp.
- Vurdere om tekniske og organisatoriske tiltak er i henhold til risikobildet og kommunens målsettinger for informasjonssikkerhet.

7. Kommunedirektørens uttalelse

Utkast til rapport ble oversendt kommunedirektøren i Bodø kommune for uttalelse 15.08.2024 med 14 dagers høringsfrist. Revisor mottok høringsuttalelse 05.09.2024 etter at høringsfristen ble forlenget med en uke. Kommunedirektøren har lagt høringssvaret direkte inn i teksten. Revisor har også vedlagt eposten med oversendelsen. Her går det fram at høringssvaret finnes på side 50 til 52. Sidetallene er forskjøvet etter sluttredigeringen og høringssvaret er fortsatt i vedlegg en, men på side 52 til 54.

I høringssvaret er det fire punkter som revisor ønsker å svare ut nærmere.

1. Sjette avsnitt, nederst på side 52.

… påstanden fra revisor om at informasjonssikkerhetsarbeidet ikke er forankret i kommunens ledelse.

Denne teksten er fra revisors vurdering (3.1.3) av revisjonskriteriet som sier at kommunen skal ha et styringssystem for sikkerhet som omfatter informasjonssikkerhet, som angir sikkerhetsmål, sikkerhetsstrategi og en sikkerhetsorganisasjon, hvor roller og ansvar framgår.

En ytterligere begrunnelse for at informasjonssikkerhetsarbeidet ikke er forankret i kommunens ledelse, er at det er store mangler i styringssystemet for sikkerhet. Når styringssystemet ikke er på plass er det vanskelig å si at det er forankret i kommunens ledelse.

2. Tredje avsnitt s. 53.

… konklusjonen blir for kategorisk og med fordel kunne vært omformulert, …

Denne teksten er knyttet til revisors vurdering på revisjonskriteriet i kapittel 4.2.3. Revisjonskriteriet sier at kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser. Revisors vurdering er at sikkerheten ikke ivaretas i anskaffelses- og utviklingsprosesser.

Det finnes rett nok eksempler på at sikkerheten er ivaretatt i noen anskaffelses- og utviklingsprosesser, men dette er unntaket. Vurderingen bygger på at sikkerhet i anskaffelses- og utviklingsprosesser ikke er satt i system og dermed overlatt til den enkelte å ta hensyn til sikkerheten.

3. Fjerde avsnitt s. 53

… her synes revisor å være bastant i sin konklusjon som med fordel kunne vært omformulert, …

Denne teksten er hentet fra revisors vurdering av revisjonskriteriet om at kommunen bør ha sentral styring med sikkerhetsoppdateringer i kapittel 4.2.9. Revisors vurdering er at kommunen ikke har sentral styring med sikkerhetsoppdateringer.

Digitaliserings- og IKT-kontoret har sentral styring med sikkerhetsoppdateringer av programmer som ligger på kommunens plattform. Fagprogrammer er spredt ut over i organisasjonen og systemansvarlige har ansvaret for sikkerhetsoppdateringer. Omkring 1/3 av dem svarer at de ikke har noen rutine for å gjennomføre sikkerhetsoppdateringer. Kun halvparten følger en felles rutine. Revisors vurdering er at det ikke er noen sentral styring

med sikkerhetsoppdateringene når omkring halvparten av de systemansvarlig ikke har noen rutine eller har laget seg sin egen.

4. 5. avsnitt s. 53.

… oppfatter det er det flere kommentarer i delkapitlene under kapittel 4 Tekniske og organisatoriske tiltak som adresserer rolle- og ansvarsdeling mellom driftsleverandør og kommunen. …

Som det står i høringsuttalelsen så har kommunen ansvaret for informasjonssikkerheten. Bodø kommune kjøper tjenester fra driftsleverandøren som er avtalt i en kontrakt. Bodø kommune må i den forbindelse følge opp kontrakten slik at de vet at de får levert det de betaler for. Det er bekymringsfullt når det i høringsuttalelsen skrives at kommunen benytte eksterne, uavhengige ressurser til å kontrollere hvorvidt leverandør gjennomfører sikkerhetsarbeidet på en god måte. For revisor ser det da ut som Bodø kommune har overlatt til eksterne å legge rammene for sikkerheten i kommunen. En del av dette bildet er også at kommunen mangler styringssystem for sikkerhet (omtalt i det første punktet over).

Tilbakemeldingene i høringsuttalelsen har ikke ført til noen endringer i rapportens innhold.

8. Referanser

Lov og forskrift

Lov om nasjonal sikkerhet (Sikkerhetsloven) LOV-2018-06-01-24. Justis- og beredskapsdepartementet

Lov om behandling av personopplysninger (Personopplysningsloven) LOV-2018-06-15-38. Justis- og beredskapsdepartementet

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) LOV-2004-06-25-988. Digitaliserings- og forvaltningsdepartementet

Forskrift om kontrollutvalg og revisjon. FOR-2019-06-17-904. Kommunal- og distriktsdepartementet

Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetssikkerhetsforskriften) FOR-2018-12-20-2053. Justis- og beredskapsdepartementet

Litteratur

KPMG, udatert. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus. KS

Nasjonal sikkerhetsmyndighet (NSM) (2020) NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0. Nasjonal Sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM), udatert. Grunnprinsipper for sikkerhetsstyring. Versjon 1. Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet, udatert. Veileder i sikkerhetsstyring. Versjon 1.

Datatilsynet (lastet ned 18.03.2024) www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

9. Vedlegg

Vedlegg 1 – Kommunedirektørens uttalelse

Hei Margrete, (cc: Hanne, Kjell, Anna og Bjørn Inge)

Vedlagt følger kommunedirektørens uttalelse. Den er i vedlegg 1 – fra side 50 til og med side 52.

bodø KOMMUNE

Med vennlig hilsen

Frode Nilsen
Digitaliserings- og IKT-sjef
Administrasjonsavdelingen

tlf. 970 33 266
frode.nilsen@bodo.kommune.no
bodo.kommune.no

BODØ2024 EUROPEAN CAPITAL OF CULTURE

Kommunedirektøren vil med dette kommentere utkast til Forvaltningsrevisjon – Bodø kommune, Informasjonssikkerhet, datert 15. august 2024.

Forvaltningsrevisjonen vurderer og konkluderer på to problemstillinger:

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

I forhold til problemstilling 1 så evalueres 9 evalueringskriterier som grunnlag for konklusjon på problemstillingen: *Revisor konkluderer med at Bodø kommune mangler et styringssystem for informasjonssikkerhet, som tilfredsstiller krav i regelverket.* Tilsvarende for problemstilling 2 så evalueres 12 evalueringskriterier som grunnlag for konklusjon på problemstillingen: *Revisor konkluderer med at Bodø kommune ikke har tilfredsstillende organisatoriske og tekniske tiltak på plass for å ivareta informasjonssikkerheten.*

Innledningsvis ønsker kommunedirektøren å påpeke at Bodø kommune, som mange andre kommuner, daglig er utsatt for ulike typer dataangrep mot kommunens digitale infrastruktur. Dette har vært en situasjon som har vedvart over flere år. I en presset økonomisk situasjon har Bodø kommune de siste årene valgt å prioritere operative tiltak hvor vi sammen med eksterne samarbeidspartnere sikrer vår digitale infrastruktur best mulig, inklusiv all den digitale informasjonen som forvaltes på plattformen. Slik kommunedirektøren vurderer det har dette vært en god og vellykket strategi som så langt har bidratt til at Bodø kommune har klart å motstå et stadig mer komplekst og utfordrende trusselbilde og unngått hendelser av alvorlig karakter. Kommunedirektøren er av den oppfatning at dette er et viktig moment å synliggjøre.

Kommunedirektøren er enig i revisor sin hovedkonklusjon i forhold til problemstilling 1 hvor det konkluderes med at Bodø kommune mangler et styringssystem som tilfredsstiller krav i regelverket. Som kommunedirektøren påpekte under oppstartsmøte 3. mai så har kommunens økonomiske situasjon de siste årene medført tøffe prioriteringer hvor mange hensyn og behov må veies opp mot hverandre. Dette har medført at flere av de gode intensjonene og målsettingene i kommunens styringsdokument «Internkontroll og informasjonssikkerhet, STYRINGSSYSTEM» ikke har vært rom for å realisere.

I forhold til problemstilling 1 finner kommunedirektøren det nødvendig å kommentere påstanden fra revisor om at informasjonssikkerhetsarbeidet ikke er forankret i kommunens ledelse. Påstanden fremkommer i siste avsnitt i kap. 3.1.3. hvor delkriteriet angående hva styringssystemet bør omfatte drøftes. Selv om det er mangler i informasjonssikkerhetsarbeidet så opplever kommunedirektøren at samtlige avdelingsdirektører har et bevisst og aktivt forhold til informasjonssikkerhetsarbeidet i kommunen. Som systemeiere kjenner avdelingsdirektørene sin rolle og sitt ansvar. Noe som de har vist i praksis gjennom flere sikkerhetsøvelser de siste årene.

Kommunedirektøren er enig i revisor sin hovedkonklusjon i forhold til problemstilling 2 hvor det konkluderes med at Bodø kommune ikke har tilfredsstillende organisatoriske og tekniske tiltak på plass for å ivareta informasjonssikkerheten. Dette følger etter kommunedirektørens oppfatning som en naturlig konsekvens av at kommunen ikke fullt ut har operasjonalisert et overordnet styringsdokument. Kommunedirektøren ønsker videre å kommentere to av delkonklusjonene under problemstilling 2 samt kommentere på overordnet nivå betraktninger knyttet til inngått driftsavtale.

Revisor konkluderer i kap. 4.2.3 at sikkerheten ikke ivaretas i anskaffelses- og utviklingsprosesser. Kommunedirektøren er av den oppfatning at de siste årene så er det et økt fokus på sikkerheten i anbudsprosessene. Slik kommunedirektøren oppfatter det skriver revisor selv i begrunnelsen at det finnes eksempler på at dette gjøres. Kommunedirektøren er derfor av den oppfatning at konklusjonen blir for kategorisk og med fordel kunne vært omformulert, eksempelvis: *Sikkerheten ivaretas ikke i tilstrekkelig grad og omfang i anskaffelses- og utviklingsprosesser*.

Revisor konkluderer i kap. 4.2.9 at kommunen ikke har sentral styring med sikkerhetsoppdateringer. Samtidig skrives det i begrunnelsen at D-IKT, som forvalter hele IKT-plattformen har jevnlige sikkerhetsoppdateringer. Disse oppdateringene utgjør det store flertallet av alle sikkerhetsoppdateringer som gjennomføres. Kommunedirektøren mener at også her synes revisor å være bastant i sin konklusjon som med fordel kunne vært omformulert, eksempelvis: *Kommunen har sentral styring av sikkerhetsoppdateringer på selve driftsplattformen, men det er en svakhet at det er fagapplikasjoner som faller utenfor styringen.*

Slik kommunedirektøren oppfatter det er det flere kommentarer i delkapitlene under kapittel *4 Tekniske og organisatoriske tiltak* som adresserer rolle- ansvarsdeling mellom driftsleverandør og kommunen. Eksempelvis skrives det i kapittel 4.2.5: *Revisor vurderer at ansvarsfordelingen mellom kommunen og driftsleverandøren er noe uklar når det gjelder sikkerheten*. Generelt vil kommunedirektøren påpeke at ved tjenesteutsetting så vil det alltid være Bodø kommune som har ansvaret for informasjonssikkerheten. Etter kommunedirektørens syn så innebærer imidlertid ikke det at Bodø kommune skal besitte detaljkunnskap knyttet til elementer som sikkerhetsarkitektur, tekniske detaljer på sikkerhetsovervåkning, backup løsning, sikkerhetskopiering mm. Noe av hensikten med tjenesteutsetting er nettopp at denne type detaljinnsikt overlates til profesjonelle aktører i markedet som har langt bedre faglige forutsetninger for å gjøre en god jobb enn en kommunal aktør. Så vil kommunen benytte eksterne, uavhengige ressurser til å kontrollere hvorvidt leverandør gjennomfører sikkerhetsarbeidet på en god måte. Sett fra kommunedirektørens ståsted så kan det synes som om revisor har et noe annet synspunkt på hvilken kompetanse det er nødvendig at kommunen selv besitter.

Avslutningsvis knyttes det noen korte innledende kommentarer til revisor sine foreslåtte tiltak. Det presiseres at disse må være gjenstand for en grundigere vurdering i organisasjonen:

- Etablere et helhetlig styringssystem for informasjonssikkerhet.
  Kommentar: Et nødvendig tiltak for å formalisere/operasjonalisere rammene for alt informasjonssikkerhetsarbeid i kommunen. En tilnærming kan være å etablere en arbeidsgruppe som gjennomgår dagens styringsdokument, oppdaterer det, legger det fram for administrativ/politisk godkjenning. Styringsdokumentet må ha realistiske målsettinger og være gjennomførbart innen de rammene som kommunen må forholde seg til.

- Sørge for å komplettere registrering av behandlingsprotokoller, herunder ferdigstiller DPIA og databehandleravtaler.
  Kommentar: Dette jobbes det godt med i dag og vil være et kontinuerlig arbeid. Mye er på plass, men det er krevende med dagens rammebetingelser å innfri dette kravet fullt ut.

- Gi ansatte opplæring i informasjonssikkerhet.
  Kommentar: Et nødvendig tiltak hvor en mulig løsning er kursing gjennom eLærings portalen til kommunen.

- Gjennomgå driftsavtalen og følge den opp.
  Kommentar: Etter kommunedirektørens syn så er driftsavtalen kontinuerlig gjenstand for oppfølging/revisjon av interne og eksterne ressurser. Imidlertid kan det med fordel iverksettes tiltak for å bedre den generelle forståelsen av avtalen i organisasjonen og hvilken relevans/rolle den har i kommunens informasjonssikkerhetsarbeid.

- Vurdere om tekniske og organisatoriske tiltak er i henhold til risikobildet og kommunens målsettinger for informasjonssikkerhet.
  Kommentar: Bodø kommune har i en årrekke vært god på å vurdere om tekniske og organisatoriske tiltak er i henhold til risikobildet. Men, i og med at det ikke foreligger et operasjonalisert styringsdokument med klare målsettinger, så må det kjøres en prosess når nytt styringsdokument er etablert og godkjent for å sikre sammenheng mellom styringsdokument og nødvendige tiltak.

Vedlegg 2 – Utledede revisjonskriterier

Ifølge forskrift om kontrollutvalg og revisjon (§ 15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhets-sikkerhetsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NMSs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

Overordnet styringssystem og rammeverk

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetssikkerhetsforskriften definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring skriver at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd: *Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.*

Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhetsstyring (NSM 2020) er overordnet for hele virksomheten og disse utfylles av grunnprinsipper for fysisk sikkerhet, IKT-sikkerhet og personellsikkerhet.

Ifølge veilederen i sikkerhetsstyring omfatter sikkerhetsstyring alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet. Sikkerhetsstyring skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Utformingen av styringssystemet for sikkerhet skal omfatte følgende prinsipper:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og prosedyrer
- Forhold til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Datatilsynet anbefaler i sin veileder om virksomhetens plikter, at det benyttes anerkjente standarder, rammeverk og veiledere som beskriver styringssystem for informasjonssikkerhet.

Sikkerhetsmål og sikkerhetsstrategi

Virksomhetssikkerhetsforskriften fastsetter krav om sikkerhetsmål i § 5. Virksomheten skal fastsette hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier for å evaluere om kravene er oppfylt.

eForvaltningsforskriftens § 15 omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan. Første ledd krever at mål og strategier for informasjonssikkerhet er beskrevet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for forvaltnings-organets internkontroll på området for informasjonssikkerhet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Kravene i personvernforordningen vil være aktuelle å innarbeide i en slik sikkerhetsstrategi.

Datatilsynet[13] skriver at sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette gjelder blant annet fordeling og avklaring av arbeidsoppgaver mellom ledelse og driftspersonell, men også beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Videre skal sikkerhetsstrategien gjøre rede for organisatoriske og tekniske strategiske valg. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene.

Sikkerhetsorganisasjon

Jamfør sikkerhetsloven § 4-1 er det er virksomhetens leder som har ansvaret for det forebyggende sikkerhetsarbeidet. I forskriften om virksomhetens sikkerhet stilles det i § 4

[13] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

krav om styringsdokument. Leder av virksomheten skal fastsette et styringsdokument som beskriver hvilke deler av sikkerhetsloven som gjelder for virksomheten, roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid og prinsipper for virksomhetens sikkerhetsarbeid. Styringsdokumentet skal gjøres kjent og tilgjengelig for blant annet alle ansatte. Virksomhetssikkerhetsforskriften § 6 definerer videre krav til roller og ansvar for det forebyggende sikkerhetsarbeidet. Det er leder sitt ansvar å fordele roller og ansvar, og at disse gjøres kjent i virksomheten.

Internkontroll

Internkontroll er hjemlet i kommuneloven § 25, der det står at internkontrollen skal være systematisk og tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren er ansvarlig for internkontrollen og 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.

Andre ledd i § 15 i eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være integrert som en del av virksomhetens helhetlige styringssystem. Tredje ledd i § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko.

I fjerde ledd bokstavene a til h, § 15, gis det eksempler på hvilke forhold sikkerhetsstrategien og internkontrollen bør adressere, herunder prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Risikovurderinger

Sikkerhetsloven § 4-2 krever at virksomheten regelmessig skal gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten, som en del av vurderingen av risiko, kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i virksomhetssikkerhetsforskriften § 12. Forskriften sier i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Personopplysninger

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs

personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

Datatilsynet har laget informasjon om pliktene en virksomhet har etter personvernregelverket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personopplysningsloven). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet[14] skriver følgende om DPIA:

> «*En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak*.»

DPIA skal som minimum inneholde:

- En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.
- En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.
- En vurdering av risikoene for de registrertes rettigheter og friheter.
- De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere stå oppført i protokollen.

Opplæring

Sikkerhetsloven definerer i § 4-1 at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Kravet om ressurser og kompetanse er videre utdypet i virksomhetssikkerhetsforskriften § 7. Forskriften krever blant annet at de ansatte som får tilgang til skjermingsverdige verdier, får tilstrekkelig kompetanse om sikkerhet og kartlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser. Veilederen fra NSM skriver at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

[14] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Datatilsynet skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne må være gitt muligheten til å etterleve dette i sitt daglige arbeid gjennom tilpasset opplæring ut fra behovet. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Hendelser

Virksomhetsforskriften § 8 sier at ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.

NSM sine grunnprinsipper for sikkerhetsstyring (versjon 1) sier at etter en uønsket hendelse bør det forebyggende sikkerhetsarbeidet i virksomheten evalueres. Virksomheten må forsikre seg om at tiltakene som er etablert fungerer etter hensikten og vurdere om hendelsen ble håndtert tilfredsstillende. NSM skriver at dette er viktig fordi:

> «*Når en hendelse er ferdig håndtert og akseptabelt sikkerhetsnivå gjenopprettet, er det viktig at virksomheten hurtig identifiserer og lærer fra det inntrufne og sørger for at konklusjoner blir gjennomgått og tatt tak i. Dersom dette ikke gjøres vil kunnskap og erfaring forsvinne, og man kan gjøre de samme feilene om igjen neste gang en uønsket hendelse oppstår. Det kan være at det oppdages nye sårbarheter, eller behov for nye eller forbedrede sikringstiltak som kan forhindre at fremtidige situasjoner oppstår.*»

På bakgrunn av redegjørelsen over, er følgende revisjonskriterier utledet for den første problemstillingen.

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

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Problemstilling 2: Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Nasjonal sikkerhetsmyndighet har utgitt en veileder om grunnprinsipper for IKT-sikkerhet for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på teknologiske og organisatoriske tiltak, og hovedfokuset er på tilsiktende handlinger.

Grunnprinsippene for IKT-sikkerhet er delt inn i fire kategorier og er gjengitt i tabellen under.

Tabell 1. Grunnprinsipper for IKT-sikkerhet.

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

Kilde: Nasjonal sikkerhetsmyndighet 2020

Identifisere og kartlegge

NSM skriver at kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i kommunen. Det er viktig at kommunen selv får oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Videre skriver NSM at risikobildet må vurderes knyttet opp til valget mellom sikkerhet og behovet for leveranser til kommunen. Det kan hende at kommunen må godta enheter med lavere sikkerhetsnivå enn ønsket, og det er derfor viktig at kommunen er bevisst på strategier som velges og vurderer de funksjonelle behovene opp mot risiko. Anbefalt tiltak fra NSM er å kartlegge enheter og programvare.

Det er også viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. En angriper har ofte som mål å øke tilgangen ved et angrep på informasjonssystemet. Mange brukere kan ha tilganger og rettigheter til systemer og tjenester de egentlig ikke har behov for. Derfor bør tilganger og rettigheter begrenses slik at skaden fra en potensiell angriper eller utro ansatt reduseres. Derfor bør kommunen kartlegge brukere og behov for tilgang.

Utledet revisjonskriterier:

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

Beskytte og opprette

NSM har et prinsipp som sier at sikkerheten i anskaffelse- og utviklingsprosesser må ivaretas. Målet med prinsippet er å minimere risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Et av prinsippene under denne kategorien er å etablere en sikker IKT-arkitektur. Et IKT-system består av mange sikkerhetsfunksjoner og ulike IKT-produkter fra ulike produsenter som skal fungere godt og sikkert sammen. Manglende kompatibilitet kan øke sårbarheten på en måte som angriperne kan utnytte. Videre skriver NSM at drift- og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, hvis ikke øker risikoen for dobbeltarbeid, menneskelige feil og flere sårbarheter. IKT-systemet bør videre deles opp i forskjellige deler avhengig av tillitsnivå for å begrense risiko.

Under prinsippet om å ivareta en sikker konfigurasjon, anbefaler NSM å etablere et sentralt styrt regime for sikkerhetsoppdatering. I dette ligger det blant annet at kommunen bør installere sikkerhetsoppdatering så fort som mulig. Videre bør kommunen ha en prioriteringsliste for oppdateringer og etablere en rutine med klare ansvarsforhold for hvor ofte oppdateringer skal utføres og hvem som er ansvarlig dersom en oppdatering ikke kan gjennomføres eller må utsettes.

NSM skriver at et av prinsippene er å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap. Et av de anbefalte tiltakene er å lage en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.

Utledet revisjonskriterier:

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

Oppdage

NSM har et prinsipp som omhandler etablering av sikkerhetsovervåkning for å overvåke og samle inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for å analysere data. Dette for at kommunen kan oppdage sikkerhetshendelser så tidlig som mulig for å minimere skadeomfanget eller forhindre hendelser. Det er viktig at kommunen har tilgang på tilstrekkelig data, siden det kan være avgjørende for at kommunen skal gjenopprette normaltilstand og hindre gjentagelse av en hendelse. NSM anbefaler derfor at kommunen etablerer sikkerhetsovervåkning.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkningen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM skriver at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

Et prinsipp til under kategorien oppdage, er at kommunen bør gjennomføre inntrengnings-tester. Kommunen bør jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

Utledet revisjonskriterier:

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

Håndtere og gjenopprette

For å forberede kommunen på håndtering av hendelser, anbefaler NSM at kommunen etablerer et planverk for hendelseshåndtering. Uten en plan og en prosess for hendelseshåndtering vil det være vanskelig for kommunen å begrense skaden og gjenopprette normal tilstand.

Ved en hendelse er det viktig at kommunen håndtere hendelsen korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt. For å få til dette er det viktig at kommunen har en plan for gjenoppretting som iverksettes i løpet av eller i etterkant av hendelsen.

Utledet revisjonskriterier:

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

Vedlegg 3 – Sikkerhetsstrategier i Bodø kommune

- Forebygge uautorisert innsyn i IT-systemene og i annen informasjon ved tilsiktede handlinger som tyveri, hacking, virusspredning osv.
- Aktivt bruke risikovurdering for å forbedre de tekniske og organisatoriske tiltakene i informasjonssystemene.
- Informasjonssystemet i Bodø kommune skal konfigureres og forvaltes slik at tilfredsstillende informasjonssikkerhet oppnås.
- Det skal tas hensyn til personvern i alle utviklingsfaser ved større endringer eller anskaffelse av nye informasjonssystemer (innebygd personvern).
- Bodø kommune skal ha fokus på personvern i digitaliseringsprosessene.
- Sørge for at det foretas en tilfredsstillende vurdering av personvernkonsekvenser (DPIA) ved innføring av nye informasjonssystemer.
- Gjennom forebyggende tiltak og kontrolltiltak sikre at kommunen produserer informasjon som er nødvendig, relevant og korrekt, samt sikre at informasjonen er tilgjengelig (for dem som skal ha den), uten ekstra ventetid og innsats.
- Opplysningene skal behandles i tråd med reglene om taushetsplikt og være beskyttet, slik at uvedkommende ikke får kjennskap til dem.
- Personer i Bodø kommune skal gis tilgang i henhold til fastsatte prinsipper for tilgangsstyring.
- Alle tilganger skal registreres i form av logger i helseregistre (inkludert elektronisk pasientjournal EPJ) og i fagsystemer.
- For å sikre sporbarhet skal det registreres i behandling hvem som har foretatt registrering, endring, retting og sletting.
- Gjennom sikkerhetstiltak sikre at personer eller teknologi i eller utenfor Bodø kommune ikke skal kunne endre registrering, endring, retting og sletting uten autorisasjon.
- Gjennom sikker identifisering sikre at personopplysninger kun blir tilgengelig for rett person.
- Personopplysninger skal være fullstendige og ajourført for behandlingen av opplysningene.
- Forholdet mellom behandlingsansvarlig og databehandleren skal være regulert i en databehandleravtale som skal sikre at personopplysninger blir behandlet i samsvar med regelverket. Dette gjelder både der kommunen er behandlingsansvarlig, men også databehandler.
- Praktisere åpenhet om hvordan kommunen behandler personopplysninger, (så lenge det ikke svekker sikkerheten).
- De registrerte skal på anmodning få innsyn og informasjon om hvilke personopplysninger kommunen behandler, hvilke sikkerhetstiltak kommunen har rundt bruken av opplysninger og hvordan personopplysningene brukes.
- Alle avvik og sikkerhetsbrudd skal registreres i Kvalitetslosen for oppfølging, korrigering og forbedring.
- Dersom sikkerhetsbruddet/avvikets art tilsier det, skal Datatilsynet og eventuelt de berørte varsles så raskt som mulig.
- Ved uønskede hendelser skal kommunen redusere konsekvenser av eventuelle feil og uhell og sikre gjenopprettelse til normalsituasjon.
- Alle ansatte i Bodø kommune skal bli gjort kjent med og etterleve gjeldende lov- og regelverk, (se pkt. 6.2 opplæring).

- Informasjonssikkerhetsarbeidet i Bodø kommune skal være et kontinuerlig forbedringsarbeid underlagt et systematisk og planlagt styringssystem.
- Kommunen skal opptre proaktivt og etablere alle nødvendige og organisatoriske og tekniske tiltak for å sikre at regelverket etterleves.
- Konfidensialitet skal gå foran behovet for tilgjengelighet (tilgang).

Salten kommunerevisjon IKS
Org.nr.: 986 655 271 MVA
post@salten-revisjon.no | salten-revisjon.no

Hovedkontor - Fauske
Postadresse: Postboks 140, 8201 Fauske
Besøksadresse: Torggata 10, 8200 Fauske

Avdelingskontor - Bodø
Postadresse: Postboks 429, 8001 Bodø
Besøksadresse: Central Atrium, Dronningensgt. 18 4.etg