Follo distriktsrevisjon

Forvaltningsrevisjonsrapport

Informasjonssikkerhet og IT-drift

Nesodden kommune

25.10/2011 RAPPORT 5/11

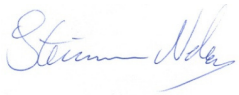
Forord

Forvaltningsrevisjon er en lovpålagt oppgave for Nesodden kommune etter Kommuneloven av 25. september 1992 med endringer av 12. desember 2003. Formålet med forvaltningsrevisjon er nedfelt i lovens § 77 nr. 4 som har følgende ordlyd:

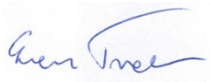
> Kontrollutvalget skal påse at kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte. Kontrollutvalget skal videre påse at det føres kontroll med at den økonomiske forvaltning foregår i samsvar med gjeldende bestemmelser og vedtak, og at det blir gjennomført systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger (forvaltningsrevisjon).

I denne undersøkelsen har Follo distriktsrevisjon vurdert informasjonssikkerhet og IT-drift i Nesodden kommune.

Prosjektet er gjennomført i perioden januar 2011 til sept 2011. Follo distriktsrevisjon vil benytte anledningen til å takke kommunens kontaktperson og øvrige ansatte i Nesodden kommune som har bistått revisjonen i forbindelse med gjennomføringen av undersøkelsen.



Steinar Neby
Revisjonssjef



Even Tveter
Prosjektleder

Innholdsfortegnelse

1 SAMMENDRAG 5

2 FORMÅL OG PROBLEMSTILLINGER 8

2.1 BAKGRUNN 8
2.2 FORMÅL OG PROBLEMSTILLINGER 8
2.3 AVGRENSNINGER 8

3 METODER OG GJENNOMFØRING 9

3.1 GJENNOMFØRING 9
3.2 DATAENES PÅLITELIGHET OG GYLDIGHET 9

4 INFORMASJONSSIKKERHET 10

4.1 REVISJONSKRITERIER 10
4.2 FAKTABESKRIVELSE 12
4.3 VURDERING 18
4.4 KONKLUSJON 20

5 IT-DRIFT 21

5.1 REVISJONSKRITERIER 21
5.2 FAKTABESKRIVELSE 23
5.3 VURDERING 29
5.4 KONKLUSJON 31

6 FLYTTING 33

6.1 FAKTA 33
6.2 VURDERING 33
6.3 KONKLUSJON 34

7 ANBEFALINGER 35

8 RÅDMANNENS UTTALELSE 36

9 REVISJONENS KOMMENTARER TIL RÅDMANNENS UTTALELSE 39

10 LITTERATURLISTE 40

1 Sammendrag

Forvaltningsrevisjonsprosjektet om informasjonssikkerhet og IT-drift i Nesodden kommune er gjennomført iht. vedtak i kontrollutvalget i Nesodden kommune. Formålet med prosjektet har vært å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard.

Undersøkelsen har vist at følgende forhold i Nesodden kommune er vurdert som tilfredsstillende:

- Nesodden kommune har utarbeidet sikkerhetsmål og sikkerhetsstrategier. Sikkerhetsorganisasjonen er også beskrevet.

- Det er etablert en sikkerhetsledelse i kommunen hvor skillet mellom rollene som utøvende og kontrollerende funksjoner er tatt hensyn til.

- Det er utarbeidet en oversikt over personregistrene i kommunen.

- Ved å ta i bruk modul for avvikshåndtering i Kvalitetslosen vil Nesodden kommune få et system for å registrere og følge opp avvik i forhold sikkerhetsbrudd.

- Alle kommunens fagsystemer har systemansvarlige. Systemsvarlig for CosDoc[1] gjennomfører jevnlig kontroll av tilgangene.

- Arbeidsdelingen innen IKT i Nesodden kommune ivaretar kravet til et skille mellom de respektive rollene innen IKT.

- Alle endringer på kommunens systemer gjøres på bakgrunn av meldinger fra systemeierne, mens IKT-seksjonen utfører endringene. Tilbakemeldingene fra avdelingene vi har snakket med tyder på at dette har fungert på en akseptabel måte.

Gjennom prosjektet er det identifisert følgende forhold som er vurdert som ikke tilfredsstillende:

- Mål og strategier er utarbeidet i august 2001 og delvis revidert i 2006. Mål og strategier er ikke gjennomgått jevnlig i tilstrekkelig grad slik regelverket tilsier.

- Rollefordeling og ansvar rundt kommunikasjonen mot Datatilsynet fremstår ikke som tilstrekkelig avklart. Revisjonen kan ikke se at meldinger til Datatilsynet er blitt sendt i tilstrekkelig grad.

- Det er ikke gjennomført jevnlig sikkerhetsrevisjon slik § 2-5 i personopplysnings-forskriften sier. Med unntak av 2010 er det gjennomført egenkontroller i avdelingene.

[1] CosDoc er et pasientjournalsystem i pleie-, omsorg- og rehabiliteringssektoren

- Det bør etter revisjonens skjønn innføres en rutine for jevnlig kontroll av tilganger på kommunens fagsystemer, tilsvarende hva som er gjort for CosDoc.

- Nesodden kommunes IKT-strategi og strategisk plan er revidert august 2006 og gjaldt fram til 2009. Disse planene er dermed ikke gyldige lengre. Det er opplyst at planverket skal revideres i sammenheng med den omorganiseringen som skal finne sted.

- Sikkerhetsutvalget har ikke fulgt opp sine oppgaver ved at det ikke er gjennomført tilstrekkelig omfang egenkontroller i 2009 og 2010, samt at det ikke er gjennomført uanmeldte sikkerhetskontroller. Utvalget har heller ikke gjennomført det antall møter i 2010 og 2011 som kommunen selv har forutsatt.

- IKT- seksjonen har ikke utarbeidet egne beredskapsplaner for alvorlige hendelser.

- Revisjonen mener at kommunen bør avklare om det er tilstrekkelig kapasitet i IKT-seksjonen og om organiseringen og tilgjengeligheten til helpdesk er tilfredsstillende.

- Driftsforstyrrelser og nedetid i kommunens systemer loggføres ikke. Revisjonen mener kommunen bør vurdere å innføre dette. Forventninger og krav til driftsstabilitet bør også avklares med de respektive avdelingene.

- Alle endringer på kommunens systemer gjøres på bakgrunn av meldinger fra systemeierne, mens IKT-seksjonen utfører endringene. Tilbakemeldingene fra flere avdelingene tyder på at dette har fungert på en akseptabel måte. Endringene som gjøres dokumenteres i et manuelt system. Revisjonen mener at dette systemet bør forbedres.

- Det er ikke ferdigstilt planer for flyttingen til nytt rådhus som inkluderer IKT. Slike planer er under utarbeidelse. Slik det blir uttrykt overfor revisjonen, mener IKT-seksjonen likevel å ha kontroll på den delen av flyttingen som vedrører IKT-systemer. IKT - seksjonen har vært førende i hele prosessen og fremholder at de har blitt hørt i de sammenhenger som de har ansett som viktige. All flytting er tenkt å skulle foregå på kveldstid og skal ikke medføre noe nedetid på kommunens systemer. Inntil det foreligger planer med tilstrekkelig robusthet for å håndtere uforutsette hendelser, er det etter revisjonens mening likevel grunn til å betrakte dette som et risikoområde som kommunen må ha fokus på.

Follo distriktsrevisjon har med bakgrunn i de funn som er gjort, avslutningsvis gitt en del anbefalinger som vi mener kan bidra til forbedringer innen informasjonssikkerhet og IT-drift.

2 Formål og problemstillinger

2.1 Bakgrunn

Kontrollutvalget fattet i møte 31. januar 2011 vedtak om at det skulle gjennomføres en forvaltningsrevisjon av Informasjonssikkerhet og IT-drift i Nesodden kommune. Prosjektet ble godkjent som sak 4/11.

2.2 Formål og problemstillinger

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard.

Følgende problemstillinger er belyst:

Informasjonssikkerhet

- Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
    - Tilfredsstiller kommunen sikkerhetsbestemmelsene i personopplysningsforskriften[2]?

IT-drift

- Er det etablert overordnede mål, retningslinjer og rutiner for IT i kommunen?
    - Følges God IT-skikk?
- Er det tilfredsstillende arbeidsdeling vedrørende IT?
- Har kommunen rutiner for å gjenoppta normal drift etter en driftsstans?
- Har kommunen rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?

Flytting

- Er det utarbeidet planer for å sikre overføringen av IT-drift ved flytting til nytt rådhus?
    - I hvilken grad har IT-avdelingen vært involvert i prosessen rundt flyttingen?

2.3 Avgrensninger

Prosjektet omfatter ikke en kartlegging av Nesodden kommunes IT-systemer, således heller ikke revisjon av de enkelte systemer. Det er ikke vurdert om informasjonssystemene er hensiktsmessige for virksomhetens behov. Kartlegging av informasjonssikkerhetsarbeidet er avgrenset til et overordnet nivå i kommunen og inkluderer av den grunn ikke de enkelte virksomheters/ansattes aktiviteter.

[2] FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger

3 Metoder og gjennomføring

Undersøkelsen er basert på en kombinasjon av analyser av utleverte dokumenter og intervjuer med personer i ulike roller knyttet til IKT- og informasjonssikkerhet i kommunen. Hensikten med dokumentanalysen er å vurdere om styringsdokumentene innen IT er tilstrekkelige i forhold til aktuelle anbefalinger (beste praksis) knyttet til IT-drift og krav i forskrift knyttet til informasjonssikkerhet. Intervjuene av ansatte og ledere innen IKT og informasjonssikkerhet er rettet mot å få en forståelse av praksis og etterlevelsen av regelverket og rutiner i kommunen.

3.1 Gjennomføring

Kontaktperson i kommunen har vært kommunens sikkerhetsansvarlige.

Revisjonen valgte ut følgende funksjoner for intervju:

- Kommunens IKT-sjef.
- Kommunens sikkerhetsansvarlig.
- Pleie- og omsorgssjef, systemansvarlig ved pleie- og omsorg.
- Helsesjef, systemansvarlige ved helseavdelingen.
- Skole- og oppvekstsjef, systemansvarlig ved skolene.

3.2 Dataenes pålitelighet og gyldighet

Kvalitetssikring av datagrunnlaget omfatter en vurdering av reliabilitet og validitet.

Begrepet **reliabilitet** beskriver analysens pålitelighet. I dette ligger at pålitelighet setter krav til nøyaktig datainnsamling og at det ikke er skjedd systematiske feil underveis i innsamlingen. Begrepet **validitet** beskriver analysens gyldighet, det vil si hvor godt det gitte materialet belyser problemstillingen i en undersøkelse.

Det er utarbeidet en intervjuguide hvor spørsmålene i guiden følger av problemstillingene som ligger til grunn for undersøkelsen.

Intervjusituasjonen gjør det også mulig å kunne oppklare misforståelser og stille oppfølgingsspørsmål, hvilket også bidrar til styrket reliabilitet. Det styrker også reliabiliteten at intervjuobjektene selv har verifisert de opplysningene de har gitt i intervjuet.

4 Informasjonssikkerhet

- Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
  - Tilfredsstiller kommunen sikkerhetsbestemmelsene i personopplysningsforskriften?

4.1 Revisjonskriterier

Av Personopplysningsloven (POL) § 13 framgår det at *" den behandlingsansvarlige*[3] *databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet men hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger".*

Av veileder til sikkerhetsbestemmelsen utgitt av Datatilsynet[4] framgår det at begrepet informasjonssikkerhet omfatter:

- Sikring av **konfidensialitet**, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene.
- Sikring av **integritet**, dvs. beskyttelse mot utilsiktet endring av opplysningene.
- Sikring av **tilgjengelighet**, dvs. å sørge for at tilstrekkelige og relevante opplysninger er til stede.

Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av planlagte og systematiske tiltak. Begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet skal legges til grunn ved sikkerhetsarbeidet.

Personopplysningsforskriften (POF) definerer nærmere hvilke krav som hviler på kommunen for at tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger finner sted:

§ 2-3 stiller krav om at det skal etableres en sikkerhetsledelse. Ansvaret for at bestemmelsene for informasjonssikkerhet følges påhviler virksomhetens daglige ledelse. Videre skal virksomheten etablere sikkerhetsmål og sikkerhetsstrategi hvor formålet, overordnede føringer, valg og prioriteringer framkommer. Ledelsen skal jevnlig gjennomgå sikkerhetsmål og strategi.

§ 2-4 stiller krav om at det skal føres en oversikt over hvilke personopplysninger som behandles. Videre kreves det at den behandlingsansvarlige gjennomfører en risikovurdering for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ved endringer av betydning for informasjonssikkerheten skal ny risikovurdering gjennomføres.

[3] For Nesodden kommune vil dette være rådmannen.
[4] Desember 2000

§ 2-5 stiller krav om at det jevnlig gjennomføres sikkerhetsrevisjon. Denne skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Resultatet av sikkerhetsrevisjonen skal dokumenteres.

§ 2-6 stiller krav om at bruk av informasjonssystemet som er i strid med fastlagte rutiner og sikkerhetsbrudd skal behandles som avvik.

§ 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarlige daglige leder.

I Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften påpekes det at det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeidet (sikkerhetsledelse) er klarlagt. Disse funksjonene er henholdsvis "utøvende" og "kontrollerende" og bør ideelt sett tillegges forskjellige medarbeidere i virksomheten. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

§ 2-10 stiller krav om fysisk sikring mot uautorisert tilgang til utstyr som brukes for å behandle personopplysninger definert i forskriften eller annet utstyr av betydning for informasjonssikkerheten. I veileder for informasjonssikkerhet for kommuner og fylker, utgitt av Datatilsynet[5], framkommer det vedrørende fysisk sikkerhet at virksomheten skal sørge for at lokaler og utstyr den benytter er forsvarlig sikret. Det skal spesielt legges vekt på de rom hvor det er plassert utstyr benyttet for behandling av sensitive personopplysninger, eller for sikring av slike.

§ 2-11 sier at det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er viktig.

§ 2-12 sier at det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgang er nødvendig. Av veileder fra Datatilsynet framgår det at det skal tas backup av personopplysninger.

§ 2-13 sier at det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Av veileder fra Datatilsynet framgår det at dette innebærer bl.a. tilstrekkelig beskyttelse mot datavirus.

På bakgrunn av det ovennevnte kan følgende kriterier legges til grunn for undersøkelsen:

- Kommunen skal ha etablert en sikkerhetsledelse som jevnlig gjennomgår sikkerhetsmål og strategi.
- Kommunen skal ha en klar organisering med etablerte ansvars- og myndighetsforhold.
- Kommunen skal ha tilstrekkelig oversikt over de personregistre som finnes og gjennomføre risikovurdering av disse.
- Kommunen skal jevnlig gjennomføre sikkerhetsrevisjon.
- Kommunen skal ha et avvikssystem for å håndtere sikkerhetsbrudd.
- Kommunen skal ha gjennomført tiltak som:

[5] TV-202:2005

- Ivaretar fysisk sikring av IKT-utstyr.
- Hindrer uautorisert innsyn i personopplysninger.
- Sikrer tilgang til personopplysninger.
- Hindrer uautorisert endring av personopplysninger.

4.2 Faktabeskrivelse

4.2.1 Organisering

IKT-seksjonen i Nesodden kommune er organisert under administrasjonsavdelingen. Seksjonen har 5 ansatte inkludert seksjonsleder (IKT-sjef).

Rådmannen har det overordnede sikkerhetsansvaret i kommunen og har ansvaret for at det utarbeides en policy og retningslinjer for IKT-sikkerhet. Dette arbeidet er i Nesodden kommune delegert til leder av sikkerhetsutvalget som er sikkerhetsansvarlig i kommunen. Sikkerhetsansvarlig er plassert som rådgiver ved rådmannskontoret. Nåværende sikkerhetsansvarlig har vært ansatt siden november 2010. Sikkerhetsutvalget skal påse og følge opp at kommunen har en forsvarlig internkontroll og at det årlig gjennomføres egenkontroller. Leder av sikkerhetsutvalget er kommunens kontaktperson mot Datatilsynet. Sikkerhetsansvarlig oppgir at hun ofte er på kommunens ledermøter slik at rollen er godt kjent blant avdelingssjefene. Alle de intervjuede lederne oppgir at de er kjent med hvem som er kommunens sikkerhetsansvarlig.

IKT-sjef har ansvaret for den driftstekniske sikkerheten av IKT-systemene. De respektive avdelingssjefene har et selvstendig sikkerhets- og kontrollansvar for de respektive avdelingers bruk av informasjonsteknologi. De er også delegert ansvaret som systemeiere for kommunens fagsystemer. Systemeierne vil være ansvarlig for sikkerheten i de enkelte systemene. Systemeier skal være bl.a. være hovedansvarlig for IKT-systemet, juridisk part i relasjon til leverandører, ansvarlig for kvaliteten på IKT-systemet, fastsette og følge opp kravet til avbruddsplan/ beredskapsplan for IKT-systemet.

4.2.2 Sikkerhetsledelse, sikkerhetsmål og strategi

Nesodden kommune har utarbeidet IKT- policy, IKT-strategi og sikkerhetsregler. Dokumentene er oppdatert pr. august 2006. Det er opplyst at sikkerhetsutvalget har fått som oppgave å oppdatere dette dokumentet. Utvalget skal rapportere til rådmannens ledergruppe.

I del 1 i *"Overordnet policy for IKT-sikkerhet"* er de forskjellige roller og ansvarsforhold rundt IKT beskrevet.

Nesodden kommune har utarbeidet *Internkontroll av informasjonssikkerhet ved behandling av personopplysninger.* Dette dokumentet er utarbeidet av Micro Basert informasjon AS i samarbeid med Nesodden kommune. Dokumentet er datert 2. august 2001. Det er opplyst at det skal jobbes med å oppdatere denne, men at dette må sees i sammenhengen med den omorganisering som skal foretas i Nesodden kommune.

I dokumentet er det angitt styrende dokumenter. Dette omfatter bl.a. sikkerhetsmål, sikkerhetsstrategi, ansvar- og myndighetsforhold, teknisk sikkerhetsløsning, og oversikt og klassifisering av personopplysninger.

I den utarbeidede strategi for IT-sikkerhet er følgende områder omtalt:

- Hva skal beskyttes?
- Organisering av informasjonssystemet.
- Partnere og leverandører
- Personellsikkerhet/ egne medarbeidere.
- Fysisk sikkerhet.
- Systemteknisk sikkerhet.
- Dokumentsikkerhet.

I dokumentet for Internkontroll av informasjonssikkerhet er det et eget punkt for prosedyrer, her framgår:

- Ledelsens gjennomgang
- Risikoanalyse
- Egenkontroll
- Avviksbehandling
- Konfigurasjonsendring
- Tilgangskontroll
- Adgangskontroll
- Dataoverføring
- Beredskapsplaner
- Dokumentsikkerhet

Som vedlegg til dokumentet foreligger dokumentasjon fra gjennomgang av IT-sikkerhet. Følgende punkter er omtalt:

- Overordnet policy for IT-sikkerhet
- Generelle retningslinjer for IT-sikkerhet
- Sårbarhetsanalyse for IT-sikkerhet generelt
- Tiltak for IT-sikkerhet generelt.
- Risikoanalyse for IT-sikkerhet for IT-systemer som behandler personsensitive data

Videre er det foretatt en risikoanalyse av 24 områder/tjenester. I analysene er det laget risikoprofiler i forhold til trusler, brudd på konfidensialitet og manglende kvalitet. Risikoen er kategorisert i forhold til konsekvens pr. 1 time, 1 dag, 1 mnd og totalverdi. Det er laget søylediagram hvor det benytter verdiene 0 = ingen konsekvens, 1 = litt skade. 2 = få konsekvenser, 3 = store hendelser og 4 = kritisk.

Videre er det gjennomført sårbarhetsanalyse for sosialtjenesten, barnevernstjenesten, helsetjenesten, pleie- og omsorgstjenesten, PP-tjenesten og rådmannen. Sårbarhetsanalysen gir en tilbakemelding på status for IT-sikkerhet på tjenesten og inneholder en vurdering av sikkerhetsnivå (kontrollnivå) sammenlignet med det ønskede sikkerhetsnivå (viktighet). Dette gir detaljert oversikt over sikkerhetsnivå innen relevante sikkerhetsområder.

For de virksomhetene der det er gjennomført sårbarhetsanalyse er det også laget rapport over tiltak. Denne inneholder tre deler:

1. Generelle tiltak.
2. Generelle tiltak på aktuelle sikkerhetsområder.
3. Detaljerte tiltaksforslag basert på områder og underområder hvor IKT-sikkerhet avviker fra anbefalt viktighetsnivå.

Som en del av kommunens internkontroll er det laget særskilte retningslinjer for IT sikkerhet i sosialtjenesten, barnevernstjenesten, fysio og ergo, helsetjenesten, PP tjenesten, overformynderi og forliksrådet. Det er her gitt retningslinjer bl.a. for hvem som gir tilganger til systemene samt passordrutiner. Det framgår av rutinen at registeransvarlig periodisk skal kjøre ut rapport med oversikt over tilgangsrettigheter for de respektive brukerne.

Det er ikke gjennomført risikoanalyse eller sårbarhetsanalyse etter 2001. Det er opplyst at det nå skal gjennomføres en ny internkontroll slik at risikoanalyse og sårbarhetsanalyse nødvendigvis må utarbeides.

4.2.3 Personregistre

Nesodden kommune har utarbeidet en oversikt over alle personregistre i kommunen. Denne er delt opp i de forskjellige avdelingene i kommunen og beskriver hva slags informasjon som er lagret. Informasjonen er gradert i forhold til om den er sensitiv eller ikke. Det er videre angitt om det er søkt konsesjon eller gitt melding til Datatilsynet. Videre er sikringstiltak og lagringssted samt omfanget av den informasjonen som er lagret, angitt. Til sammen har kommunen registrert 52 manuelle og maskinelt lagrede arkiv av personregistre.
Disse opplysningene er angitt for i alt 52 registre. Dette gjelder både manuelle arkiv og data lagret maskinelt.

I forbindelse med utarbeidelsen av *Internkontroll av informasjonssikkerhet ved behandling av personopplysninger* er det sendt meldinger og søknader til Datatilsynet 24. januar 2002. Sikkerhetsansvarlig har opplyst at hun ikke har særskilt oversikt over hva som er sendt av meldinger og søknader etter denne tid. Ansvarsforhold rundt dette i forhold til hvem som gjør hva oppfattes ikke som avklart. Dette samsvarer med de opplysninger som lederne også har gitt.

Av instruks for IT sikkerhetsansvarlig fremgår det at sikkerhetsansvarlig er kommunens kontaktperson mot Datatilsynet i korrespondanse, konsesjonssøknader, innføring av nye retningslinjer, etc. Sikkerhetsansvarlig skal ha komplette kopier av alle aktuelle konsesjoner.

Av Overordnet IKT-policy framgår det at alle IKT-systemer og organisatoriske enheter skal i utgangspunktet gjennomgå en risikoanalyse. Risikoanalysen skal avdekke hvilke enheter som skal gjennomgå en sårbarhetsanalyse. Sårbarhetsanalysen skal danne grunnlag for å fremme forslag til tiltak for å bedre IKT-sikkerheten for de aktuelle IKT–systemer eller organisatorisk enhet. Det er viktig å ha rutiner for å etablere, vedlikeholde og revidere sikkerhetsnivå. Som det er omtalt i punkt 4.2.2 er det ikke gjennomført noen dokumentert risikoanalyse siden 2001.

Det er også viktig å ha rutiner for å holde oversikt over alle risikoprofiler til IKT-systemer og organisasjonsenheter.

4.2.4 Sikkerhetsrevisjon

Det er ikke framkommet opplysninger om at det er foretatt sikkerhetsrevisjon av IT i Nesodden kommune verken av sikkerhetsansvarlig, IKT-seksjonen eller de virksomhetene som er intervjuet. Det er opplyst at det skal gjennomføres en oppdatering av *"Internkontroll av informasjonssikkerhet ved behandling av personopplysninger"*. Dette arbeidet skal startes opp høsten 2011 etter at kommunens omorganisering er gjennomført. Det vil bli lagt opp til at mye av arbeidet skal gjøres av de enkelte avdelinger selv.

Av instruks for sikkerhetsansvarlig framgår det at det skal utføres uanmeldte sikkerhetskontroller i løpet av året i tillegg til planlagt egenkontroll innen områdene:

- Registeransvar på kommunens sosialsystem
- Registeransvar på kommunens barnevernssystem
- IT-driftsansvar
- Systemansvar for fagsystem som benytter sensitive personopplysninger
- Der hvor det er usikkert om sikkerhetsreglene blir overholdt.

Det er utarbeidet et skjema for "egenkontroll" hvor alle avdelinger skal ta stilling til flere kontrollområder. Dette gjelder bl.a.:

- Rutinegjennomgang
- Påloggingsrutiner
- Låserutiner
- Plassering av skriver
- Sikkerhetskopiering
- Oppdatering av programvare
- Passord
- Konfidensielt materiale
- Sikring av Pc
- Kontroll med besøkende
- Sletterutiner
- Gjennomgang av beredskapsplan
- Ansvars- og myndighetsforhold
- Opplæring

Egenkontrollen er gjennomført årlig i perioden 2002-2009. For 2010 er det ikke gjennomført egenkontroll. Sikkerhetsansvarlig har gjennomgått de avgitte egenkontrollene for 2009 og avgitt et notat til sikkerhetsutvalget og rådmannens ledergruppe hvor hver enkelt av de innleverte egenkontrollene er gjennomgått. Det går også fram av notatet at det etter diverse purringer fortsatt mangler rapportering fra fem avdelinger i 2009.

Sikkerhetsansvarlig har opplyst at hun er i gang med å revidere egenkontrollskjemaet og planen var å få sendt dette ut i løpet av mai 2011, men pga. sykdom er dette ikke gjort. Skjemaet vil bli gjennomgått med avdelingssjefene for å sikre en felles forståelse for hvordan dette skal fylles ut. De gjennomførte intervjuer med avdelingssjefene viser også at det er et behov for en revidering av den egenkontrollen som skal gjennomføres.

I forbindelse med innføringen av samhandlingsreformen[6] skal Nesodden kommune ta i bruk Helsenett. For at kommunen kan ta i bruk dette må den dokumentere at den tilfredsstiller kravene i "Normen". Helsedirektoratet har utarbeidet 52 faktaark om sikkerhet som må tilfredsstilles. Det er nedsatt en arbeidsgruppe i kommunen som skal gjennomgå dette. Det er opplyst at det da må gjennomføres nødvendige risikovurderinger av avdelingene.

4.2.5 Avviksbehandling

Sikkerhetsansvarlig har oppgitt at det ikke er meldt om avvik innen IKT siden hun begynte i stillingen i november 2010. Kvalitetslosen som er i ferd med å innføres i kommunen inneholder en egen modul for avvikshåndtering som skal brukes.

Det er utarbeidet *rutine for intern varsling av kritikkverdige forhold i Nesodden kommune.* Kritikkverdige forhold er definert som "*forhold som er i strid med lov, forskrift, reglementer kommunens vedtatte etiske reglement, eller alminnelige etiske standarder som det er en bred tilslutning til i samfunnet"*. Det er videre beskrevet hvordan det skal varsles og hvem som skal varsles.

4.2.6 Sikring av informasjon og tilgangskontroll

Kommunens IKT-systemer driftes lokalt med egen serverpark. All backup kjøres på datarom på Nesoddtunet. Backup av backupen lagres på tape på datarom i rådhuset. Det er opplyst at det er om lag 1200 ansatte i Nesodden kommune som har tilgang til kommunens systemer. Alle kommunens IKT-systemer driftes sentralt av IKT-seksjonen. Det er opplyst at det er avdelingssjefene som er systemeiere av fagsystemene. Dette kan delegeres der det er hensiktsmessig.

Av punkt 3 i overordnet IKT-policy framgår det at *IKT-sikkerhet i Nesodden kommune innebærer iverksettelse av nødvendig sikkerhetstiltak for å redusere sårbarheten til Nesoddens kommunes informasjonsbehandling og for å være best mulig forberedt på å håndtere eventuelle feil og uhell, dvs. sikre at:*

- *Informasjonen ikke blir kjent for uvedkommende, dvs. at den kun er tilgjengelig for autoriserte personer og prosesser.*
- *Informasjonen er fullstendig, korrekt og à jour og et resultat av autoriserte og kontrollerte aktiviteter.*
- *Informasjonen er tilgjengelig når det er behov for den for autoriserte personer, grupper og prosesser.*

Av punkt 4 i dokumentet framgår det bl.a. at IKT–sikkerhetspolicyen skal danne fundament og stille krav til at det forefinnes retningslinjer innen:

- Tilgangskontroll
- Kommunikasjonssikkerhet
- Fysisk sikkerhet

[6] En reform av helse- og sosialsektoren

Del 3 av overordnet policy og IKT strategi inneholder *Regler, skjemaer og maler for IKT- og dokumenthåndtering i Nesodden kommune.* I denne inngår en sikkerhetsplakat for ansatte i Nesodden kommune. Denne inneholder 13 viktige sikkerhetsregler. Det er også i dokumentet omtalt hvordan behandling og lagring av informasjon skal gjøres

Alle fagsystemer ligger på kommunens servere. Programmene ligger på "sikker" sone og det er ikke mulig å kopiere informasjon over til andre programmer. Backup foretas av alle kommunens systemer. IKT- seksjonen er lokalisert uten gjennomgangstrafikk i kommunehuset. Døren inn til seksjonen er til enhver tid låst slik at uvedkommende ikke har tilgang til seksjonens lokaler.

Alle fagsystemer har utnevnte systemansvarlige. Det er de systemansvarlige som har ansvaret for å gi tilganger og vedlikeholde de tilganger som er gitt. Systemansvarlig for CosDoc[7] har oppgitt at det hver måned blir sendt ut liste over hvem som har tilgang til systemet og hvilke tilganger som er gitt til journalansvarlige. Denne går gjennom de tilsendte listene og melder tilbake hvis det er ting som ikke stemmer. Det er utarbeidet egen prosedyre for dette. Det er den journalansvarlige som bestemmer hvem som skal ha tilganger i systemet. Dette meldes på eget skjema til systemansvarlig. Systemansvarlig opplyser videre at det er laget mange forskjellige "profiler" i forbindelse med tilganger slik at ved endringer trenger man ikke å gå inn å gjøre endringer på den enkelte. Ved nye behov lages nye profiler.

System ansvarlig for CosDoc anser at man har god oversikt og kontroll over de gitte tilgangene.

Helseavdelingen benytter seg av tre fagsystemer:

- CosDoc, ti ansatte er brukere, sjefsfysioterapeut er journalansvarlig, pleie- og omsorgsavdelingen er systemeier og systemansvarlig.
- FAMILIA, barnevernsleder er systemansvarlig. Det er 11 brukere av dette systemet og det er barnevernsleder som administrerer alle tilganger.
- Winmed[8], ledende helsesøster er systemansvarlig, det er ca 20 brukere av dette systemet.

Med unntak av CosDoc, som Pleie- og omsorgsavdelingen har oppfølging av, foretas det ingen spesiell tilgangskontroll av avdelingens systemer i de undersøkte avdelingene. Det er opplyst at det er få brukere av systemene og at det har vært en stabil arbeidsstokk de siste årene. Det anses derfor at på bakgrunn av dette at de ansvarlige har god oversikt over de tilganger og identer som er delt ut.

Skolene benytter seg av Visma skoleadministrasjon. Skole- og oppvekstsjef er systemeier mens systemansvarlig er ansatt på skolekontoret. Systemet er basert på "roller" og de definerer hvilke tilganger man skal ha. Skolene har bl.a. bare tilgang til sin egen skole. Det er skolene selv som administrerer brukere, mens systemansvarlig administrerer "rollefordelingen". Det er opplyst at det ikke foretas noen tilgangskontroller.

På sykehjemmet er det egne skrivere på alle vakttrom. Disse er koblet opp mot lokal pc. Det er i tillegg kode på skriver som gjør at man må være fysisk til stede for å få utskrift.

[7] CosDoc er et pasientjournalsystem.
[8] Winmed er pasientjournalsystem.

I forbindelse med utarbeidelse av individuell opplæringsplan har alle skolene egne pc-er som brukes til dette. De utarbeidede planene blir automatisk overført og lagret på "sikker sone" hvert 30minutt.

4.3 Vurdering

Nesodden kommune har utarbeidet dokumentene "IKT-policy, IKT-strategi og sikkerhetsregler" og dokumentet Internkontroll av informasjonssikkerhet ved behandling av personopplysninger. Dokumentene omhandler informasjonssikkerheten i kommunen.

Det er utarbeidet sikkerhetsmål og sikkerhetsstrategi i august 2001. Videre er sikkerhetsorganisasjonen og ansvarsforhold beskrevet. Sikkerhetsbestemmelsene stiller krav til gjennomgang av sikkerhetsmål og sikkerhetsstrategi jevnlig. Ledelsen skal kontrollere at disse er i samsvar med kommunens behov og eventuelt oppdatere mål, strategi og organisering. Nesodden kommune har således ikke fulgt bestemmelsen om en jevnlig gjennomgang. Deler av målstrategi og organisering er imidlertid omtalt i den utarbeidede IKT-policy fra 2006. Det er opplyst at dokumentene skal gjennomgås og oppdateres. Sikkerhetsmål og sikkerhetsstrategi vil da følgelig bli oppdatert.

Det er viktig at mål og strategier for informasjonssikkerhet og IKT revideres i takt med både kommunens utvikling og utvikling innen IKT, slik at dokumentene er oppdaterte i forhold til både risikoområder innen IKT og de behov man ser at kommunens videre utvikling krever.

Kommunens ansvarsforhold rundt IT sikkerhet er omtalt i kommunens IKT-policy fra 2006, Rådmannen har det overordnede ansvaret. Ansvar for utarbeidelse av policy og retningslinjer for IKT-sikkerhet er delegert til sikkerhetsansvarlig som også er leder for sikkerhetsutvalget. Etter revisjonens vurdering er det tatt hensyn til at det skal være etablert en sikkerhetsledelse samt at det skal være et skille mellom utøvende og kontrollerende funksjoner.

Nesodden kommune har utarbeidet en oversikt over alle personregistre i kommunen slik forskriftens § 2-4 krever. Vi vil imidlertid bemerke at det skal gjennomføres nye risikovurderinger og kartlegging av sannsynlighet og konsekvens i de tilfeller det oppstår endringer av betydning for informasjonssikkerheten. Det ble sendt felles søknader og meldinger til Datatilsynet 24. jan 2002 i forhold til de personregistre kommunen hadde på det tidspunktet. Sikkerhetsansvarlig har arkivert disse søknadene og meldingene. Søknader og meldinger gitt til Datatilsynet etter denne tid har ikke sikkerhetsansvarlig oversikt over, det revisjonens inntrykk er at rollefordelingen rundt kommunikasjonen mot Datatilsynet ikke er tilstrekkelig avklart.

Av sikkerhetsansvarliges instruks framgår det at denne skal være kontaktperson mot Datatilsynet og ha kopi av alle søknader og meldinger som er sendt. Skolesjefen har opplyst at det er sendt søknad til Datatilsynet i forbindelse med at de tok i bruk nytt skoleadministrasjonssystem, men sikkerhetsansvarlig har ikke kopi av denne søknaden. Av § 31 i personopplysningsloven framgår det at det skal gis ny melding til Datatilsynet etter 3 år selv om det ikke har skjedd endringer. Nesodden kommune bør således gjennomgå oversikten over alle personregistre og sørge for at søknader og meldinger til Datatilsynet blir semdt slik loven krever. Rolleavklaringer må også gjøres internt og kopi av søknader og meldinger må lagres hos sikkerhetsansvarlig. Det er etter revisjonens syn viktig at Nesodden kommune har

tilstrekkelig oversikt over de personregistre som finnes i kommunen og at disse blir håndtert slik Datatilsynet har forutsatt.

Av § 2-5 i personopplysningsforskriften framgår det at det jevnlig skal gjennomføres sikkerhetsrevisjon. Sikkerhetsansvarlig har opplyst at det ikke har vært gjennomført en slik revisjon i hennes tid, og hun er heller ikke kjent med at dette er blitt gjort siden 2001. Av sikkerhetsansvarliges instruks framgår det også at det skal gjennomføres uanmeldte sikkerhetskontroller i løpet av året i tillegg til planlagt egenkontroll. Etter revisjonens oppfatning er det er viktig at det foretas jevnlig sikkerhetsrevisjon slik at eventuelle avvik kan avdekkes og rettes opp.

Det er gjennomført egenkontroller i alle år med unntak av 2010. Det er dog ikke alle avdelingene som gjennomførte denne i 2009. Det er opplyst at nytt egenkontrollskjema er under utarbeidelse, samt at det er planlagt å gjennomgå dette med avdelingsledere. Revisjonen ser det som positivt at det vil bli foretatt en revidering av skjemaet og at man vil involvere avdelingsledere i forhold til gjennomføringen av dette.

Det anses som positivt at Nesodden kommune skal ta i bruk modulen for avvikshåndtering i Kvalitetslosen. Dette gjør at man kan få en ensartet håndtering av avvik og det vil også gjøre det lettere å ha oversikt over de avvik som foreligger også innenfor IKT-området. Det er opplyst at det til nå ikke er meldt noen avvik innenfor dette området. Dette kan tyde på at de ansatte ikke har et tilstrekkelig bevisst forhold til hva slike avvik kan være. Det vil derfor etter vårt syn være viktig å etablere en bevisst og ensartet holdning blant de ansatte til hva som kan være avvik inne IKT området slik at eventuelle sikkerhetsbrudd kan bli avdekket og lukket.

Revisjonen ser det som positivt at det er truffet tiltak for å ivareta den fysiske sikringen av kommunens serverpark. Alle kommunens IKT-systemer driftets lokalt og ligger på kommunens servere. Det gjennomføres også backup på kommunens systemer.

Vår gjennomgang viser at det gjennom overordnet IKT-policy er laget overordnede mål for hvordan man skal redusere sårbarheten til Nesodden kommunes informasjonsbehandling. Den utarbeidede IKT-policy var imidlertid bare gjeldene fram til 2009, det er opplyst at oppdatert versjon nå skal utarbeides.

Alle fagsystemene har systemansvarlige som har ansvaret for å gi tilganger og vedlikeholde disse. Systemansvarlig for CosDoc har oppgitt at det hver måned gjennomgås liste over de forskjellige tilganger. Det er utarbeidet mange profiler slik at brukerne bare har de tilganger som det er behov for ut i fra arbeidsoppgavene. Etter vårt syn er dette med på å ivareta kravene til å hindre uautorisert innsyn samt å sikre tilgangen til de personopplysninger som ligger i dette programmet. For de andre fagsystemene vi har gjennomgått foreligger det ingen slik rutine. Systemeierne har oppgitt at de har god kontroll på de tilganger som er gitt med bakgrunn av at det er en stabil arbeidsstokk. Etter vårt skjønn bør det også for de andre fagsystemene innføres tilsvarende rutine som for CosDoc, slik at man jevnlig foretar en gjennomgang av hvem som har tilgang til de aktuelle systemene. Man vil da til enhver tid ha sikkerhet for at det ikke er personer som har tilgang til personopplysninger som ikke skal ha dette. Selv om arbeidsstokken er stabil kan det også forekomme at behovet for de forskjellige tilgangene vil endre seg. Det er også oppgitt at sensitive personopplysningen ligger på sikker sone slik at det ikke er mulig å kopiere dette over i andre programmer, noe som også er med på å hindre at sensitive personopplysninger kommer på avveie.

Revisjonen ser det også som positive tiltak at det er satt opp skrivere med koder på sykehjemmene slik at papirer her ikke vil "ligge og slenge". Revisjonen ser det som positivt at skolene har lagt til rette for at utarbeidelse av individuelle opplæringsplaner blir håndtert på en sikker måte.

4.4 Konklusjon

Sikkerhetsledelse, sikkerhetsmål og strategi

Sikkerhetsmål og sikkerhetsstrategier er utarbeidet. Sikkerhetsorganisasjonen er også beskrevet. Mål og strategier er imidlertid utarbeidet i august 2001, og deler av mål og strategier er sist revidert i 2006. Mål og strategier er da følgelig ikke gjennomgått jevnlig i tilstrekkelig grad slik regelverket tilsier.

Det er tatt hensyn til at det skal være etablert en sikkerhetsledelse samt at det skal være et skille mellom utøvende og kontrollerende funksjoner.

Personregistre
Det er utarbeidet en oversikt over personregistrene i kommunen. Det er imidlertid viktig å foreta nye risikovurderinger i tilfeller der det er vesentlige endringer. Revisjonen mener at rollefordeling og ansvar rundt kommunikasjonen mot Datatilsynet ikke er tilstrekkelig avklart. Meldinger til Datatilsynet er ikke blitt gitt i tilstrekkelig grad.

Sikkerhetsrevisjon
Det er ikke gjennomført jevnlig sikkerhetsrevisjon slik § 2-5 i personopplysningsforskriften krever. Med unntak av 2010 er det gjennomført egenkontroller i avdelingene. Nytt egenkontrollskjema er planlagt utarbeidet.

Avviksbehandling
Ved å ta i bruk modul for avvikshåndtering i Kvalitetslosen vil Nesodden kommune få et system for å registrere og følge opp avvik i forhold sikkerhetsbrudd. Forutsetningen for at dette skal fungere er at de ansatte får tilstrekkelig informasjon og har en ensartet og er bevisst i forhold til hva som skal rapporteres som avvik.

Sikring av informasjon og tilgangskontroll
Alle kommunens fagsystemer har systemansvarlige som har ansvaret for å gi tilganger og vedlikeholde disse. Systemsvarlig for CosDoc gjennomfører jevnlig kontroll av tilgangene og dette er med på å sikre at kravene til å hindre uautorisert innsyn blir ivaretatt. Det bør etter vårt skjønn innføres tilsvarende rutine for kommunens øvrige systemer slik at man til enhver tid kan være trygg på at det ikke er personer som har tiganger til systemer de ikke skal. Sensitive personopplysninger ligger på sikker sone på kommunens servere slik at dette ikke kan kopieres over i andre programmer. Dette er også med på å hindre at sensitive opplysninger kan komme på avveie. Sykehjemmene og skolene har også lagt opp rutiner for å håndtere utskrifter av personopplysninger på en tilfredsstillende måte.

5 IT-drift

- Er det etablert overordnede mål, retningslinjer og rutiner for IT i kommunen?
  - Følges God IT-skikk
- Er det tilfredsstillende arbeidsdeling vedrørende IT?
- Har kommunen rutiner for å gjenoppta normal drift etter en driftsstans?
- Har kommunen rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?

5.1 Revisjonskriterier

5.1.1 Overordnede mål, retningslinjer og rutiner

ISACA[9] har publisert anbefalinger for God IT-skikk. I denne undersøkelsen har vi lagt til grunn publiseringer og anbefalinger fra denne foreningen.

God IT-skikk og COBIT[10] *anbefaler* at en etablerer IT-strategi/planer og at disse er forankret i og bygger opp under kommunens mål og planer. I tillegg bør en ha konkrete handlingsplaner og investeringsplaner for hvordan de overordnede strategiene skal nås.

God IT-skikk anbefaler at det foreligger dokumentasjon som viser samtlige IT-systemer og sammenhengen mellom disse. Dokumentasjonen bør inneholde en overordnet informasjon om systemene. En samlet dokumentasjon av et system skal for øvrig bestå av: [11]

- **Systemdokumentasjon**: IT-systemet skal beskrives tilstrekkelig detaljert til at forsvarlig systemforvaltning (vedlikehold og videreutvikling) muliggjøres.

- **Brukerdokumentasjon**: Dokumentasjonen skal på en oversiktlig og lettfattelig måte beskrive systemet med tilhørende manuelle rutiner slik det arter seg for brukeren.

- **Driftsdokumentasjon**: Dokumentasjonen er en beskrivelse av systemets oppbygging og driftsmønster for å sikre korrekt drift av IT-systemet, driftsmessig vedlikehold og stabilitet.

5.1.2 Arbeidsdeling

Statskonsult[12] og KS[13] *anbefaler* at IT-organisasjonen klart skiller mellom rollene: styring av IT-området, bestiller av IT-løsninger og leverandør av IT-løsninger. Innholdet i disse rollene er:

[9] Information Systems Audit and Control Association (ISACA) er en verdensomspennende forening for IT-styring og kontroll, sikkerhet, kontroll og revisjon av informasjonsteknologi
[10] Control Objectives for Information and Related Technology (COBIT) er utviklet av ISACA og IT Governance Institute (ITGI) og gir anbefalinger for god IT-skikk.
[11] Anbefaling til God IT-skikk (nr. 1) Dokumentasjon av IT-systemer 2001
[12] IKT i det offentlige 2002

- **Styringsrollen:** Styringsrollen omfatter den overordnede strategiske planleggingen, koordineringen og styringen som er nødvendig for å følge opp IT-virksomheten.

- **Bestillerrollen:** Systemeier er en bestiller av funksjonalitet og IT-løsninger. (Det største brukermiljøet på bestillersiden er normalt systemeier.) Bestillerrollen omfatter ansvaret for brukerkrav/funksjonelle krav.

- **Leverandørrollen:** Leverandøren skal, på oppdrag fra kunden, levere spesifiserte IT-løsninger og IT-tjenester. Leverandørrollen skal ha ansvar for å fremskaffe den funksjonalitet som er ønsket. Dette omfatter leveranse av maskiner, basis programvare, standardsystemer, utviklingsprosjekter, system- og programmeringstjenester og tjenester til drift og forvaltning samt brukerstøtte. En IT-avdeling er ofte tildelt en vesentlig del av ansvaret for leverandørrollen, selv om det kjøpes inn ressurser fra eksterne leverandører på en del av oppgavene. COBIT anbefaler at det bør være etablert en IT-organisasjon med klare roller og nødvendig myndighet til å utøve ansvaret for IT i kommunen. Klare roller med beskrivelse av oppgaver og ansvar bør også foreligge.

5.1.3 Driftskontinuitet

God IT-skikk anbefaler at det etableres beredskapsplaner som ivaretar kontinuiteten i driften ved alvorlige/katastrofale hendelser.

God IT-skikk anbefaler at driftsforstyrrelser logges og at det informeres til systemeiere og brukere ved driftsbrudd. Det bør også settes et nivå for når en forstyrrelse er så alvorlig at katastrofe/beredskapsplanen settes i verk.

5.1.4 Endringshåndtering

God IT-skikk definerer en rekke aktiviteter en virksomhet må iverksette for å sikre en forsvarlig gjennomføring av endringer som påvirker drift av IT-systemene, herunder tiltak for å sikre at alle endringer blir gjennomført på en effektiv og kontrollert måte, til rett tid og med forventet resultat. Dette forutsetter at alle endringer er autorisert, planlagt, prioritert, risikovurdert, dokumentert, testet og godkjent. God IT-skikk anbefaler at en etablerer retningslinjer, prosedyrer og instrukser for endringshåndtering.

5.1.5 Kriterier

På bakgrunn av det ovennevnte legges følgende kriterier til grunn for undersøkelsen:

- Det skal være utarbeidet IT-strategi/-planer og mål for IT-drift i kommunen.
- Det skal være et klart skille mellom roller innen organisasjonen.
- Det skal være planer som ivaretar driftskontinuiteten.
- Det skal være retningslinjer og prosedyrer for endringshåndtering, samt dokumentasjon fra kommunens IT-systemer

[13] Verktøykasse for IKT-planlegging 2004 Analyse av IKT organiseringen, Kommunenes Sentralforbund TN 7

5.2 Faktabeskrivelse

5.2.1 Overordnede mål og strategier

Nesodden kommunes IKT-policy og IKT-strategi er utarbeidet august 2006 og gjelder 2006-2009. Strategisk plan for IKT utgjør del 2 av denne. Dokumentet er revidert i forhold til det opprinnelige dokumentet fra 2001.

Nesodden kommunens IKT-visjon er:

Nesodden kommune skal bidra aktivt til at alle tilsatte gis mulighet for digital samhandling og kommunikasjon på en sikker, enkel og effektiv måte.

Dette betyr:

Nesodden kommune skal fremstå som en arbeidsgiver som bidrar til å utvikle og effektivisere elektroniske tjenester, internt i egen organisasjon og eksternt til innbyggere og andre samarbeidspartnere. Nesodden kommune skal bidra til bedre digital samhandling på tvers av fagavdelinger og forvaltningsnivåer. IKT skal være et av kommunens viktigste verktøy for å nå vedtatte mål, og skal bidra til å realisere gevinster knyttet til bruk av elektroniske hjelpemidler

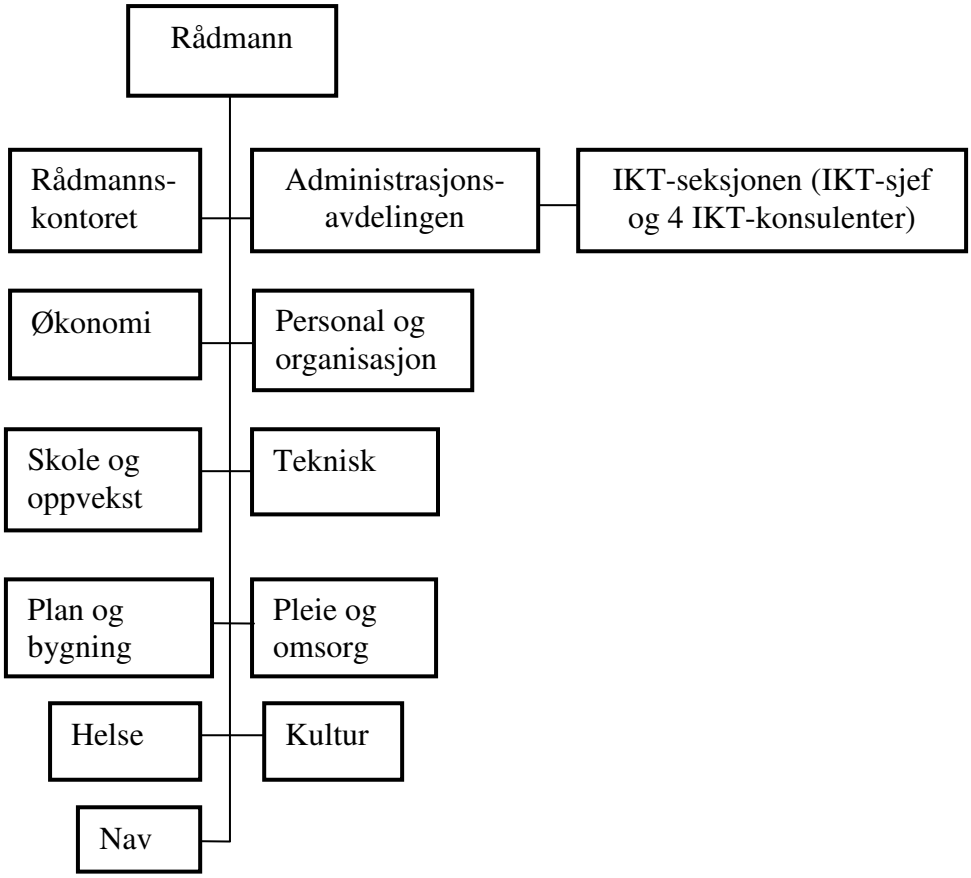
IKT-strategien skal legge vekt på:

- Bedre kommunal service (kvalitet og kvantitet)
- Raskere saksbehandling
- Bedre, sikrere og raskere kommunikasjon (eksternt og internt)
- Bedre arbeidsmiljø
- Bedre styring og ledelse

Nesodden kommune er i ferd med å foreta en omorganisering. Det er opplyst at kommunens rutiner således må gjennomgås Alle kommunens prosedyrer og rutiner skal legges inn i kommunens kvalitetssystem.

5.2.2 Organisering og ansvarsdeling

IKT-seksjonens organisatoriske tilknytning:



Styringsrollen

Rådmannen har det overordnede ansvaret og er ansvarlig for at det utarbeides en overordnet IKT-strategi og at kommunen har en forsvarlig sikkerhetspolitikk.

Nesodden kommune har etablert et IKT-utvalg. Utvalget skal bidra til å utarbeide sentrale strategier og retningslinjer for bruk av IKT. IKT-utvalget er rådførende ved prioritering av IKT-prosjekter og fordeling av midler/ ressurser.

Utvalget skal bestå av:
- Avdelingssjef administrasjonsavdelingen + IKT-sjef
- Personalsjef
- 2 representanter fra enhetene
- Tilsattes representant

Utvalget skal velge en sekretær og det avholdes minimum 4 møter pr år.

Utvalget skal påse og følge opp at kommunen har en forsvarlig internkontroll og at det gjennomføres årlige egenkontroller. Sikkerhetsansvarlig er leder av dette utvalget. Denne personen er også kommunens kontaktperson mot Datatilsynet.

Det er opplyst at siste møtet i utvalget var i januar 2010, hvor de gjennomførte egenevalueringene for 2009. De avvik som det var meldt om er vurdert og kommentert av sikkerhetsansvarlig. Gjennomgangen i sikkerhetsutvalget ble senere lagt fram for rådmannens ledergruppe.

Leverandørrollen

Administrasjonsavdelingen skal fungere som det utførende leddet, rådgiver og som faglig støtte. Avdelingen har ansvaret for vedlikehold og oppfølging av tekniske standarder samt anskaffelser og drift. IKT-utvalget skal fungere som en referansegruppe og skal bidra med hensiktsmessige prioriteringer.

IKT-sjef har opplyst at det i utgangspunktet ikke er fordelt spesielle oppgaver på den enkelte konsulent men at den enkeltes kompetanse vil styre dette i noen grad. Det er utarbeidet stillingsbeskrivelser men disse er ikke oppdatert. Etter IKT-sjefens oppfatning burde det vært en større grad av "spesialisering" internt med en klarere fordeling av oppgaver med overlapping. For å få dette til må seksjonen imidlertid styrkes. Oppgavene er i noen grad fordelt (muntlig). De siste årene har seksjonens oppgaver økt ved at organisasjonen har vokst og de tekniske løsningene blir mer avanserte, uten at ressursene er økt.

Bestillerrollen

Avdelingssjefene er systemansvarlige (eier av dataprogram). Systemeierfunksjonen kan delegeres men dette skal meldes IKT-seksjonen.

Brukerne

Brukernes ansvar er også beskrevet. Her framgår det at de skal rette seg etter rutiner og sikkerhetsregler som gjelder for de systemene som benyttes. De ansatte har plikt til å gjøre seg kjent med rutiner, regelverk og det sikkerhetsnivå som gjelder.

Det er videre beskrevet ansvarsområder og oppgaver for IKTpersonalet, systemadministrator og superbrukere. IKT-sjef og IKT-konsulenters ansvarsområde og kompetanse er også beskrevet. IKT-helpdesks oppgaver og ansvarsforhold er også beskrevet i dokumentet. Det framgår her at alle henvendelser angående driftsproblemer, samt faglige IKTspørsmål, skal rettes hit. Helpdesk skal være bemannet i arbeidstiden.

Alle systemer skal ha en systemadministrator som skal ha god kunnskap om aktuelt fagprogram. Systemadministrator skal enten være avdelingssjef eller seksjonsleder men oppgaven kan delegeres når dette er hensiktsmessig. Systemadministrators rolle og oppgaver er beskrevet. Det går videre fram at administrator skal være bindeledd mellom den sentrale IKT-enheten og programvareleverandør og den enkelte avdeling når det gjelder programvare. Funksjonen som superbruker framgår av stillingsbeskrivelsen. I tillegg til administratorene på programmene skal det være superbrukere. Disse skal ha god kjennskap til generelle programmer i tillegg til eventuelle fagprogrammer. Superbrukerne skal være knyttet til den avdelingen de er tilsatt.

Opplæring

De tilsatte må gis mulighet til en kvalitativt god opplæring i fagsystemene som er nødvendige for å utføre sitt arbeid på en effektiv måte. Avdelingssjefene er ansvarlig for å kartlegge behov for opplæring og kompetanseutvikling. Personal- og organisasjonsavdelingen, i samarbeid med skole- og oppvekstavdelingen og administrasjonsavdelingen, er ansvarlig for organisering og gjennomføring av opplæring.

Administrasjonsavdelingen/IKT-sjef er ansvarlig for å utarbeide opplæringsplan for IKT-konsulentene. Avdelingssjefene i samarbeid med programleverandørene er ansvarlig for opplæring av systemadministratorer.

Alle nyansatte skal ha tilbud og plikt til å gjennomføre nødvendig grunnopplæring. De enkelte avdelinger skal ut fra eget behov selv ta initiativ til utvikling og opplæring knyttet til bestemte oppgaver. På kommunens intranett er det en egen fane for nyansatte hvor alle relevante instrukser for nyansatte er tilgjengelig.

Alle de intervjuede avdelingene har oppgitt at de anser at de har tilstrekkelig med kompetanse internt på sine fagsystemer. Pleie- og omsorgsavdelingen oppgir at det gjennomføres jevnlige kurs for ansatte i forhold til personopplysninger og journalføring. Det er både kapasitet og tekniske løsninger til å gjennomføre dette internt. Det er gjennomført kurs både på dag-, kvelds- og nattestid slik at alle vaktskift er i varetatt. Systemansvarlig har bl.a. gjennomført kurs med informasjonssikkerhet i forhold til samhandlingsreformen.

Avdeling for skole og oppvekst oppgir at de selv foretar intern opplæring på sine systemer. Man har tilgang på kursrom i forbindelse med aktuell opplæring. Kommunens skole-sekretærer har et eget faglig nettverk hvor en er superbruker i denne forbindelsen.

Helseavdelingen har oppgitt at den har hatt en stabil arbeidsstokk og derfor ikke hatt behov for større opplæringstiltak.

IKT-sjef oppgir at kompetansen i IKT-seksjonen kunne vært noe bedre, og at man har liten tid til å utvikle kompetanse. Konsekvensen av dette er å kjøpe konsulenttjenester ved behov. Konsulentene brukes bl.a. for å løse problemer som IKT-seksjonen selv ikke har tid eller kompetanse til å gjøre. Det er inngått en rammeavtale vedrørende kjøp av IKT-bistand. Dersom ikke IKT-seksjonen blir tilført økte ressurser er IKT-sjef av den oppfatning at det må påregnes økt bruk av konsulenter.

5.2.3 Driftskontinuitet/ driftssikkerhet

Måling og evaluering av kontinuitet

IKT-seksjonen har ikke systemer for å måle oppetid på kommunens IKT-systemer. De avdelingene som det er gjennomført intervju med oppgir at de selv ikke registrerer eventuelle nedetid på systemene. Alle har imidlertid oppgitt at de ikke opplever at det er mye nedetid på kommunens IKT-systemer. Pleie og omsorg har imidlertid opplyst at man har hatt problemer med nedetid flere helger og i ferie og høytid. IKT har ikke vaktordning utenom ordinær

arbeidstid, slik at hjelpen med å få i gang systemene har vært tilfeldig. Pleie- og omsorgs-avdelingen oppgir at den ser et klart behov for å få avklart roller ved uventet nedetid. Dette vil være særlig viktig i forbindelse med innføringen av helsenett[14] til sykehus. Normen som kommunene må forholde seg til i forbindelse med innføringen av helsenett anbefaler at systemet senest skal opp etter tre timer nedetid eller at kommunen må lage en forsvarlig prosedyre.

Det er pr i dag ikke noe overvåkningssystem av kommunens servere. I forbindelse med flytting til nytt rådhus ligger det inne i budsjettene et overvåkningssystem som vil overvåke bl.a. fukt, brann, strøm, innbrudd og temperatur. IKT-sjef er av den oppfatning at man da vil få et tilfredsstillende og fullverdig serverrom.

Driftsikkerhet

Kommunens sikkerhetsutvalg og sikkerhetsplan skal ivareta det offentliges og innbyggernes krav til sikring av personopplysninger.

Det skal kun gis autorisasjon for de programmer som den enkelte er avhengig av i sitt daglige arbeid, og behov skal meldes skriftlig til IKT-seksjonen. Det skal videre etableres backup-rutiner for alle systemer.

IKT-seksjonen skal sørge for at alle IKT-systemene som administreres og driftes av Nesodden kommune er tilgjengelige i normalarbeidstiden.

Den enkelte avdelingssjef er ansvarlig for å ha utarbeidet en beredskapsplan for situasjoner som kan oppstå som følge av brudd på den elektroniske kommunikasjonen. Dette gjelder for de spesifikke fagsystemmer. Planene skal inneholde rutiner for eventuelt manuelt arbeid som må utføres som en følge av at dataprogrammer og/eller elektronisk utstyr midlertidig er satt ut av drift.

Når det gjelder beredskapsplan for standardisert/ felles programvare og utstyr, skal dette utarbeides av IKT-seksjonen.

Nesodden kommune har utarbeidet en risiko- og sårbarhetsanalyse. Denne er utarbeidet i mars 2009 og tar utgangspunkt i mulige kritiske hendelser som kan oppstå. Ved langvarig brudd i kommunens datasystemer er det satt opp hvem som skal varsles, tiltak som skal gjennomføres og informasjon.

Det er ikke utarbeidet egne beredskapsplaner verken i de avdelingene hvor vi har gjennomført intervjuer eller for IKT-seksjonen. Pleie- og omsorgsavdelingen har utarbeidet manuelle rutiner i forbindelse med nedetid på sitt fagsystem. Dette gjør at de kan håndtere inntil en ukes nedetid. Avdeling for skole og oppvekst og avdeling for helse har ikke utarbeidet spesielle rutiner for håndtering av nedetid. Begge avdelingene har henvist til at nedetid ikke vil ha livsviktige konsekvenser. Helseavdelingen oppgir at eventuell nedetid vil medføre en del merarbeid i ettertid, men at man i hovedsak vil få løst sine oppgaver. Man har bl.a. et manuelt arkivsystem på alle klienter. Skole har oppgitt at det vil være mest kritisk dersom systemene er nede når eksamen nasjonale prøver avholdes.

[14] Nettverk for elektronsk samhandling i helse- og omsorgssektoren i Norge

IKT-sjef er av den oppfatning at den enkelte avdeling bør stille krav om driftsstabilitet slik at IKT-seksjonen kan dimensjoneres i forhold til summen av de kravene som stilles. IKT-sjef oppgir videre at rollefordelingen mellom IKT-seksjonen og de andre avdelingene føles noe uklar. Man har ikke ressurser nok til å understøtte alle nye behov, som for eksempel mobiltelefoner. Vanlig drift og vedlikehold tar det meste av ressursene til seksjonen. IKT-sjef har nå utarbeidet en "serviceavtale" mellom IKT-seksjonen og de respektive systemeierne. Formålet med denne er å avklare og definere ansvarsforhold, plikter og rettigheter mellom partene. IKT-sjef oppgir at en av de store utfordringene framover blir å tilfredsstille behovene og kravene til lagringsplass og tilgjengelighet som bare vil øke framover.

IKT-seksjonen gjennomfører ingen logging av "nede tid" på kommunens systemer, men har inntrykk av at brukerne er fornøyde. Det oppleves at det har vært en forbedring av stabiliteten på kommunens systemer de siste årene. Det er ikke installert nødstrøm for kommunens servere. Det er imidlertid nødstrøm på kommunens backupsystemer. All backup kjøres på datarommet på Nesoddtunet. Det er opplyst at backup av backupen lagres på tape i datarom på rådhuset.

I forbindelse med flytting til nytt rådhus er det planlagt at det også vil bli installert nødstrømsaggregat i kommunens serverrom.

I forbindelse med planlagt nedetid på kommunens servere er det opplyst at det informeres via kommunens intranett. De intervjuede avdelingene har alle oppgitt at det har vært tilfredsstillene varsling i forbindelse med planlagt nedetid.

Helpdesk

Det er opplyst at ved telefonhenvendelser vil førstelinjekontakt være servicesenteret som da vil registrere saken som IKT vil ta tak i. Det er bevisst gjort et valg om at alle telefon-henvendelser skal gå gjennom servicesenteret for å frigjøre ressurser i IKT-seksjonen. Tanken er at man skal få luket bort en del "enkle" problemer som avdelingene kan løse internt med den kunnskapen de har der. Alle henvendelser vil få et saksnr. og blir loggført i et eget verktøy(system) for oppfølging og tilbakemelding til brukerne. Melding vil også kunne gis pr. mail eller på webskjema.

Både pleie- og omsorgsavdelingen og helseavdelingen har opplyst at de er lite tilfreds med dagens helpdeskløsning. Man anser å ha så god kompetanse på fagsystemet at det ikke er tilfredsstillende først å måtte ta kontakt med servicesenteret.

Avdeling for skole har oppgitt at den til nå i liten grad har benyttet seg av helpdesk, da den har hatt god kontakt direkte med IKT-seksjonen.

5.2.4 Endringshåndtering, dokumentasjon

Infrastruktur, programvare og utstyr

Administrasjonsavdelingen er ansvarlig for at alt utstyr og programvare registreres.

All felles programvare skal standardiseres, og det er avdelingssjefen som skal vurdere behovet for tilgang til programvare for tilsatte i egen avdeling. Det er videre gitt en beskrivelse av hvordan man håndterer felles systemer som sak/arkiv-system og hvem som skal ha tilgang til fagsystemer. Alle ansatte skal ha mulighet for tilgang til PC på sitt arbeidssted med tilgang til internett/intranett inkludert. På tjenestesteder der dette ikke er mulig skal det være plassert minimum en PC med tilstrekkelig tilganger som de ansatte kan benytte. Alt utstyr skal standardiseres så langt dette er mulig.

Endringshåndtering

IKT-sjef har opplyst at det ikke er fastsatt rutiner vedrørende endringshåndtering. Alle oppgraderinger foretas "live". Ved større oppgraderinger kjøres det ekstra backup. I forbindelse med flyttingen til nytt rådhus vil det være større mulighet for å opprette et testmiljø. De intervjuede avdelingssjefene har opplyst at alle oppgraderinger i regi av IKT har fungert tilfredsstillende.

IKT-sjef har opplyst at det er et manuelt system hvor det dokumenteres endringer som gjøres på systemene. Etter IKT-sjefens oppfatning bør man ha et bedre system enn det som er gjeldende i dag. I IKT-seksjonens inventarregister registreres all systemdokumentasjon som ikke vedrører fagsystemene. Systemeierne har ansvar for egne fagsystemer. Det er opplyst at systemdokumentasjonen for fagsystemene er tilgjengelig i de enkelte systemene.

5.3 Vurdering

Overordnede mål og strategier

Nesodden kommune har utarbeidet en IKT-strategi i august 2001 som er revidert august 2006 og gjaldt fram til 2009. Strategisk plan for IKT er utarbeidet oktober 2000 og revidert i august 2006. Kommunens IKT-strategi og strategiske plan er således utgått på dato. Det er imidlertid opplyst at denne nå skal revideres og da i sammenheng med den omorganiseringen som skal finne sted. Revisjonen ser det som viktig at det blir foretatt en full gjennomgang av kommunes IKT-strategi og at det utarbeides en oppdatert versjon av denne som gjenspeiler de nye faktiske forhold. Den opprinnelige planen ser imidlertid ut til å være tilstrekkelig forankret i Nesodden kommune.

Organisering og ansvarsdeling

Når det gjelder rolle og ansvarsforhold registrer revisjonen at Nesodden kommune foruten rådmannens overordnede ansvar har etablert en struktur hvor avdelingsledere er systemeiere. De har dermed bestillerrollen mens IKT-seksjonen utfører oppgavene. I tillegg er det lagt en del kontrolloppgaver på sikkerhetsansvarlig og kommunens IKT-utvalg. Denne rolledelingen reflekterer de anbefalinger regelverket gir. IKT-utvalget har imidlertid ikke fulgt opp sine oppgaver ved at det skal påse at kommunen har en forsvarlig internkontroll og at det gjennomføres årlige egenkontroller. Det er heller ikke gjennomført uanmeldte sikkerhetskontroller i avdelingene. Siste møte i utvalget er avholdt i januar 2010, slik at de følgelig heller ikke har fulgt den møtehyppigheten som er bestemt.

IKT-sjef har påpekt at det burde vært en større grad av spesialisering internt i seksjonen, men for å få dette til må seksjonen styrkes med ressurser. Den enkeltes kompetanse vil imidlertid styre fordelingen av oppgavene noe. IKT-sjef har også etterlyst en klarere rollefordeling mot de andre avdelingene, samt at også avdelingene bør stille krav om driftsstabilitet. Dette for at IKT-seksjonen kan dimensjoneres i forhold til servicenivået som er ønskelig.

Revisjonen ser det som positivt at det nå er utarbeidet en serviceavtale mellom IKT-seksjonen og de andre avdelingene for å avklare rollefordelinger og forventninger. Det bør forventes at de uklarheter som har oppstått vil bli avklart i en slik avtale. Revisjonen er også enig med IKT-sjef at forventninger til driftsstabilitet og oppetid bør avklares.

Det er flere avdelinger som ikke er tilfreds med helpdeskløsningen til kommunen. IKT har opplyst at løsningen med servicesenteret som førstelinjekontakt er etablert for å spare ressurser. En avdeling har oppgitt at den har hatt problemer med nedetid på sitt IT-system i forbindelse med helger og ferier, og at IKT ikke har hatt tilstrekkelig vaktordning slik at hjelpen med å få i gang systemet har vært tilfeldig.

IKT-sjef har også oppgitt at kompetansen i IT-avdelingen kunne ha vært noe bedre og at avdelingen må kjøpe eksterne tjenester der den selv ikke har tid eller kompetanse til å løse alle oppgavene selv. Man har også hatt liten tid til å utvikle kompetansen internt.

Etter vårt skjønn bør Nesodden kommune vurdere disse innspillene for å se om bemanningen i IKT-seksjonen er tilpasset de behov og krav som avdelingene har. Kompetansemessig vil det også være en stor fordel for IKT-seksjonen å ha mulighet for tilstrekkelig kunnskapsmessig overlapping for viktige funksjoner slik at den vil være mindre sårbare i forbindelse med fravær av enkeltpersoner. Utvikling av tilstrekkelig intern kompetanse er viktig for å få dette til. Med innføringen av helsenett vil det også blir stilt krav til driftsstabilitet, noe som vil påvirke kapasiteten som er nødvendig i IKT-seksjonen.

Revisjonen har også registrert at det er utarbeidet stillingsbeskrivelser i IKT-seksjonen uten at disse er oppdatert eller aktivt i bruk.

Driftskontinuitet/ driftssikkerhet

IKT-seksjonen har ikke utarbeidet egne beredskapsplaner for hvordan den skal håndterere alvorlige hendelser. Det er viktig med slike planer for å sikre at kommunen er tilstrekkelig forberedt for alvorlige hendelser og kan redusere konsekvensene av disse. God IT-skikk anbefaler også at det etableres beredskapsplaner for ivaretakelse av driften ved alvorlige hendelser. I Nesodden kommunes risiko og sårbarhetsanalyse framgår det hvem som skal varsles og hvilken informasjon som skal gis ved langvarige brudd i kommunens datasystemer. Konkrete tiltak for å gjenoppta driften er ikke omtalt. Etter revisjonens oppfatning bør beredskapsplaner utarbeides. Revisjonen registrerer at det er planer for å utarbeide beredskapsplaner for standardiserte/ felles programvare og utstyr.

Driftsforstyrrelser og nedetid på kommunens IT systemer logges ikke av IKT-seksjonen. IKT-seksjonen er av den oppfatning at stabiliteten er blitt bedre de siste årene. Ingen av de spurte avdelingene opplever at kommunens systemer er mye nede. Revisjonen er likevel av den oppfatning at det bør vurderes å loggføre driftsforstyrrelser, da mindre driftsforstyrrelser over tid også kan gå ut over effektiviteten ved avdelingene. Loggingen gir også informasjon og tilbakemelding både til IKT-seksjonen og til systemeiere og brukere. De spurte avdelingene

har oppgitt at de i tilstrekkelig grad blir informert ved planlagte nedetid. Revisjonen ser det som positivt at det i forbindelse med flytting til nytt rådhus vil bli installert med et nytt oppdatert overvåkningssystem av kommunens serverpark.

Nesodden kommune har også rutiner for backup. Backup lagres på Nesoddtunet hvor det også er nødstrømsaggregat.

Endringshåndtering, dokumentasjon

Når det gjelder endringer på systemene har IKT-sjef opplyst at alle endringer gjøres direkte mot brukerne. Ved større endringer kan dette innebære en risiko for driftskontinuiteten, IKT-sjef har opplyst at de i slike tilfeller kjøres ekstra backup. Endringer på systemer gjøres som oftest av IKT-seksjonen på grunnlag av meldinger fra systemeierne. Dette samsvarer med God IT-skikk ved at det er den som har ansvaret for systemene som autoriserer endringene. Tilbakemelding fra de avdelingene som det er gjennomført intervju med viser at det ikke har vært store problemer i forbindelse med de oppgraderinger som har blitt gjort. De endringer som gjøres arkiveres i et manuelt system. Revisjonen har registrert at IKT-sjefen mener det er behov for et bedre system. Når det gjelder systemdokumentasjon så ligger dokumentasjon for fellessystemer i et eget inventarregister. For de respektive fagsystemer er det oppgitt at system- og brukerdokumentasjon er tilgjengelig i systemene. Det vil også være tilgjengelig brukerstøtte fra leverandørene av fagsystemene.

5.4 Konklusjon

Overordnede mål og strategier

Nesodden kommunens IKT-strategi og strategisk plan er revidert august 2006 og gjaldt fram til 2009. Disse planene er dermed utgått på dato. Det er opplyst at planverket skal revideres i sammenheng med den omorganiseringen som skal finne sted. Den opprinnelige planen synes imidlertid å ha en forankring i kommunen.

Organisering og ansvarsdeling

Det er et klart skille mellom de respektive rollene innen IKT.

Sikkerhetsutvalget har ikke fulgt opp sine oppgaver ved at det ikke er gjennomført tilstrekkelig egenkontroller i 2009 og 2010 samt at det ikke er gjennomført uanmeldte sikkerhetskontroller. Utvalget har heller ikke gjennomført det antall møter i 2010 og 2011 som kommunen har forutsatt.

Nesodden kommune bør avklarer om det er tilstrekkelig kapasitet i IKT-seksjonen og om organiseringen og tilgjengeligheten til helpdesk er tilfredsstillende.

Driftskontinuitet/ driftssikkerhet

IKT-seksjonen har ikke utarbeidet egne beredskapsplaner ved alvorlige hendelser, dette bør utarbeides. Det er imidlertid en egen hendelse i kommunens risiko og sårbarhetsanalyse som vedrører langvarig brudd i kommunens datasystemer hvor det fremgår hvem som skal varsles.

Driftsforstyrrelser og nedetid i kommunens systemer loggføres ikke, etter vårt skjønn bør det vurderes å innføre dette. Forventninger og krav til driftsstabilitet bør også avklares med de respektive avdelingene.

Endringshåndtering, dokumentasjon

Alle endringer på kommunens systemer gjøres på bakgrunn av meldinger fra systemeierne, mens IKT-seksjonen utfører endringene. Tilbakemeldingene fra avdelingene revisjonen har intervjuet tyder på at dette har fungert på en akseptabel måte. Endringene som gjøres dokumenteres i et manuelt system. Systemdokumentasjonen for fellessystemer ligger i eget inventarregister, mens brukerdokumentasjon for fagsystemene er tilgjengelig i de respektive systemene.

6 Flytting

6.1 Fakta

IKT-sjef har pr. september 2011 opplyst at han er meget tilfreds med hvordan prosessen rundt flyttingen til nytt rådhus ser ut til å bli. IKT vil få tilgang til bygget og serverrommet rundt 1. desember, mens resten av kommune administrasjonen vil flytte inn ca. 1. mars 2012.

Nesodden kommune vil i samarbeid med OPAK utarbeide en flytteplan. Denne vil inneholde en del angående IKT og det vil være IKT som utarbeider denne delen.

IKT har fått påvirke plassering av serverrom i det nye rådhuset slik at dette blir slik de ønsker. Det vil også bli installert nødstrømsaggregat. Kjøling og brannslokking vil også bli tilfredsstillende. Det vil også bli adgangsbegrensninger i det nye serverrommet.

Kommunens nye rådhus er av en slik størrelse at det krever en del nytt IKT-utstyr. I og med at IKT får tilgang til bygget på et langt tidligere tidspunkt enn resten av kommunen vil dette utstyret kunne monteres og testes uten at det påvirker den daglige driften. Alt av nødvendig skap og kabler vil da også monteres.

IKT-seksjonen har også faset ut noe gammelt utstyr bl.a. ved migrering av fysiske servere til virtuelle. I følge IKT-sjef vil dette forenkle flyttingen.

Når alt nytt utstyr er montert og testet vil man flytte det resterende utstyret i etapper og dele opp kritisk utstyr. All flytting er planlagt til å gjøres på kveldstid slik at det ikke skal bli noe nedetid i forbindelse med flyttingen. Man vil flytte deler av utstyret slik at man til en hver tid vil ha nettet oppe. Man vil også kunne drifte nettet fra det nye serverrommet i nytt rådhus slik at alt kan være på plass før resten av kommunen vil flytte. Det er også opplyst at man vil kritisk gå igjennom backup før flytting av kritiske servere slik at man er sikre på å ha en 100 % backup.

6.2 Vurdering

Revisjonen registrerer at IKT-sjef er svært tilfreds med planlagt prosess rundt flyttingen. Slik flyttingen er tenkt lagt opp skal det ikke bli noe nedetid på kommunens systemer i prosessen. Revisjonen synes det er betryggende at IKT får tilgang til bygget på et så tidlig tidspunkt og dermed får tid til å til å teste og flytte kommunens utstyr i god tid før resten av kommunen skal inn i bygget.

Revisjonen registrerer at det foreløpig ikke er utarbeidet en plan for flyttingen. Inntil det foreligger planer med tilstrekkelig robusthet for å håndtere uforutsette hendelser, er det etter revisjonens mening grunn til å betrakte dette som et risikoområde som kommunen må ha fokus på.

6.3 Konklusjon

Det skal utarbeides planer for flyttingen før denne gjennomføres. IKT vil være en del av planene. Foreløpig er slike planer ikke utarbeidet. IKT-seksjonen har vært førende i hele prosessen og har blitt hørt i de sammenhenger som de har ansett som viktige. All flytting er planlagt til kveldstid og vil ikke medføre noe nedetid på kommunens systemer.

Inntil det foreligger planer med tilstrekkelig robusthet for å håndtere uforutsette hendelser, er det grunn til å betrakte dette som et risikoområde som kommunen må ha fokus på.

7 Anbefalinger

På bakgrunn av de forhold som fremkommer i rapporten foreslår Follo distriktsrevisjon følgende tiltak som kan bidra til forbedringer innen informasjonssikkerhet og IT-drift:

1. Sikkerhetsmål og sikkerhetsstrategi bør oppdateres og kommunen bør sørge for at disse jevnlig blir oppdatert.

2. IT-strategi og mål for IT-drift i kommunen bør oppdateres og revideres.

3. Beredskapsplaner i IKT-seksjonen for håndtering av alvorlige hendelser bør utarbeides.

4. Innføre rutine om å kontrollere gitte tilganger i kommunens fagsystemer jevnlig der dette ikke gjøres i dag.

5. Sikkerhetsrevisjon og uanmeldte sikkerhetskontroller bør gjennomføres jevnlig.

6. Egenkontroller bør gjennomføres årlig. Nytt kontrollskjema bør forankres hos avdelingslederne.

7. Oversikt over personregistre bør kvalitetssikres og kommunen må sørge for at det blir sendt søknader og meldinger til Datatilsynet i henhold til kapittel 6 i Personopplysningsloven.

8. Sikkerhetsansvarlig bør ha komplette kopier av søknader og meldinger til Datatilsynet. I tillegg anbefales at interne rollefordeling mot Datatilsynet avklares.

9. Forventninger og krav til driftsstabilitet og oppetid bør avklares med de respektive avdelinger, samt at logging av nedetid bør vurderes.

10. Helpdesk-funksjonen og kapasiteten i IKT-seksjonen bør vurderes.

8 Rådmannens uttalelse

Nesodden kommune
Organisasjon og tjenesteutvikling

Follo distriktsrevisjon ved Even Tveter

Midlertidig unntatt offentlighet
Off.lova § 13 Opplysningar underlagde teieplikt

Deres ref:	Vår ref:	Arkivkode:	Dato:
	11/3300-3 - 12/843	630, &13	12.01.2012

Rådmannens uttalelse til forvaltningsrevisjonsrapport om Informasjonssikkerhet og IT-drift i Nesodden kommune

Rådmannen er tilfreds med informasjon om prosjektets hensikt og metoden revisjonen har benyttet. Med økt elektronisk behandling av personopplysninger i en rekke fagsystemer og Samhandlingsreformen, med Normens krav til informasjonssikkerhet, stilles det svært strenge krav til personvern og informasjonssikkerhet i offentlig forvaltning. Det er et omfattende og tidkrevende arbeid å oppdatere styringsdokumenter og prosedyrer for gjennomføring og internkontroll for dette viktige området.

Kommunen er nå i innspurten av en stor og gjennomgripende omstilling av organisasjonen, samtidig som vi bygger og etablerer oss i nytt kommunehus. Dette er aktiviteter som medfører endrede forutsetninger for informasjonssikkerhet og IT-drift. Forvaltningsrevisjonsrapporten foreligger derfor midt i en overgangsfase.

Etter gjennomgang av forvaltningsrapporten med de anbefalinger den inneholder, har rådmannen vurdert iverksetting av følgende tiltak:

- Oppdatering av sikkerhetsmål og sikkerhetsstrategi.
  Arbeidet er godt i gang og et utkast er utarbeidet. Det er et omfattende og krevende arbeid, så det vil ta noe tid før dokumentet er ferdig.

- Oppdatering av IT-strategi og mål for IT-drift.
  Ved flytting til nytt kommunesenter har det vært nødvendig å bygge om kommunens IKT infrastruktur og etablere nytt serverrom, som er det sentrale serverrommet for hele kommunen. Mye utstyr skal flyttes og monteres i nytt rom. Dette krever ressurser og må prioriteres for at kommunen skal ha en fremtidig sikker drift, og ikke få avbrudd i forbindelse med etableringen i nytt kommunehus.

  På bakgrunn av dette, vil det først være hensiktsmessig å starte arbeidet med en

Adresse: Postboks 123 1451 NESODDTANGEN
Telefon: Telefaks: E-post: postmottak@nesodden.kommune.no
Bankkonto: 1603.07.37958 Org.nr.: 944 383 565

oppdatering av IT-strategi og mål for IT drift, etter innflytting i Tangenten, som er planlagt til mars 2012.

- Utarbeiding av beredskapsplaner for IKT.
  Beredskapsplaner for IKT vil bli utarbeidet etter flytting til Tangenten og basert på erfaring med drift i Tangenten.

- Sikkerhetsansvarlig skal utarbeide rutine for jevnlig kontroll av tilgang til fagsystemer innen 1. mars i år. Systemeier er ansvarlig for fagsystemet og systemansvarlig er ansvarlig for å gjennomføre kontroller.

- Sikkerhetsrevisjon og uanmeldte sikkerhetskontroller er delegert til sikkerhetsansvarlig og det skal utarbeides plan for gjennomføring av dette arbeidet i løpet av 2012.

- Egenkontroll vil bli gjennomført innen 1. mars og nytt egenkontrollskjema skal utarbeides og forankres hos lederne i løpet av 1. halvår 2012. Systemeier har ansvar for egenkontroll og sikkerhetsansvarlig følger opp kontrollen.

- Oversikt over personregistre bør kvalitetssikres og kommunen bør sørge for at det blir sendt meldinger til Datatilsynet ihht personopplysningsloven, kap. 6. Sikkerhetsansvarlig er ansvarlig for oppdatering av personregisteroversikt og skal ha kopi av alle meldinger til Datatilsynet. Virksomhetslederne skal melde til sikkerhetsansvarlig. Prosedyre som sikrer at sikkerhetsansvarlig får alle meldinger som skal sendes Datatilsynet, samt rolleavklaring vil bli utarbeidet.

- Det inngås samarbeidsavtaler mellom virksomheter som systemeiere og IKT for drift av fagsystemer. Avtalene inneholder blant annet avklaring av ansvarsfordeling mellom systemeier og IKT, rollefordeling og forventet responstid ved nedetid.

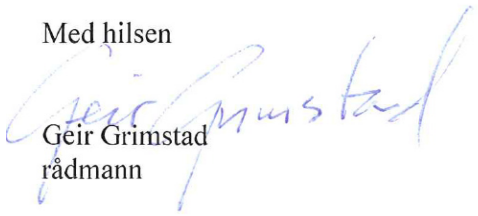
  Det er budsjettert midler i 2012 til implementering av system for overvåking av servere og nettverk. Systemet loggfører nedetid og avdekker driftsforstyrrelser på et tidligere tidspunkt, noe som vil kunne korte nedetid. Systemet er planlagt implementert 3. kvartal 2012. IKT har nylig implementert "System operation manager", et system som håndterer endringer, brukerstøtte og dokumentasjon av dette.

- Kapasiteten ved IKT og Helpdesk-funksjonen evalueres i forbindelse med omorganiseringen "Nye Takter" og følges opp i tråd med evaluering og justering av den nye organiseringen.

- Når Tangenten tas i bruk i mars, har IKT designet og etablert infrastruktur og testet denne, så flyttingen til Tangenten vil medføre svært liten risiko for driftsstans i IT-systemer. Det eneste som ikke kan flyttes i forkant er telefonlinjer, som teleoperatør er ansvarlig for å levere.

Rådmannen takker Follo distriktsrevisjon for en god og grundig rapport med konkrete anbefalinger. Anbefalingene vil være til stor hjelp for kommunen i vårt kvalitetsutviklingsarbeid knyttet til informasjonssikkerhet og IT-drift og oppfattes derfor som nyttig.

Med hilsen



Geir Grimstad
rådmann

9 Revisjonens kommentarer til rådmannens uttalelse

Revisjonen ser det som positivt at rådmannen vil iverksette konkrete tiltak i tråd med rapportens anbefalinger. Revisjonen har ikke ytterligere kommentarer til rådmannens svar.

10 Litteraturliste

Lov:

- Lov om behandling av personopplysninger (personopplysningsloven) 1.1.2001

Forskrift:

- Forskrift om behandling av personopplysninger (personopplysningsforskriften) 1.1.2001
- Datatilsynet (2000) Sikkerhetsbestemmelsene i personopplysningsforskriften - med kommentarer

Dokumenter fra Nesodden kommune:

- Tiltak for IT-sikkerhet, 2001
- Sårbarhetsanalyse, 2001
- IKT- policy, IKT-strategi og sikkerhetsregler, 2006
- Internkontroll av informasjonssikkerhet ved behandling av personopplysninger, 2001
- Regler for IKT og dokumenthåndtering – Bruk av internett og e-post for tilsatte i Nesodden kommune.
- Sikkerhetsplakat for Nesodden kommune
- Regler, skjemaer og maler for IKT- og dokument håndtering i Nesodden kommune.
- Oversikt over personregistre per. 01.01.10.
- Notat behandling av egenkontrollskjema i rådmannens ledergruppe/ skjema egenkontroll
- Rutine for varsling av kritikkverdige forhold i Nesodden kommune
- Varslingsskjema intern varsling.
- Avtaledokument - Serviceavtale mellom Systemeier og IKT-seksjonen

Annet:

- Anbefalinger til God IT-skikk (GITS) (nr. 0, 1 og 3)
- COBIT – Control Objectives for Information and Related Technology
- Datatilsynet (2000) Sikkerhetsbestemmelsene i personopplysningsforskriften - med kommentarer
- Datatilsynet (2005) Veileder i informasjonssikkerhet for kommuner og fylkeskommuner