Follo distriktsrevisjon

Forvaltningsrevisjonsrapport

Informasjonssikkerhet og IT-drift

Oppegård kommune

24. JANUAR 2007 **RAPPORT 1/2007**

Forord

Forvaltningsrevisjon er en lovpålagt oppgave for Oppegård 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:

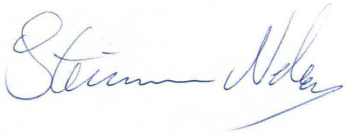
> Kontrollutvalget skal påse at kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte. Kontrollutvalget skal videre påse at det føres kontroll med at den økonomiske forvaltning foregår i samsvar med gjeldende bestemmelser og vedtak, og at det blir gjennomført systematiske vurderinger 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 Oppegård kommune. I rapporten drøftes vesentlige funn i tilknytning til problemstillingene og det gis anbefalinger som kan bidra til at Oppegård kommune kan ivareta oppgavene tilknyttet IT på bedre måter.

Prosjektet er gjennomført i perioden september 2006 til januar 2007. Follo distriktsrevisjon vil benytte anledningen til å takke kommunens kontaktperson IKT-leder Leif Nateid og øvrige ansatte i Oppegård kommune som har bistått revisjonen i forbindelse med gjennomføringen av undersøkelsen.

Prosjektet er gjennomført av rådgiver Ole Anders Sandtrøen.

Undersøkelsen ble vedtatt av kontrollutvalget i Oppegård kommune 30. august 2006.



Steinar Neby
revisjonssjef

Ole Anders Sandtrøen
prosjektleder

24.1.2007

Innholdsfortegnelse

1 Sammendrag

Forvaltningsrevisjonsprosjektet om informasjonssikkerhet og IT-drift er gjennomført i henhold til vedtak i kontrollutvalget i Oppegård kommune 31. august 2006.

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard. Konklusjonene i rapporten er delt opp i områdene informasjonssikkerhet og IT-drift.

Undersøkelsen har avdekket mangler i forhold til kravene i lov og forskrift når det gjelder informasjonssikkerhet. Revisjonen har funnet at det ikke er gjennomført sikkerhetsrevisjon. Sikkerhetsmål, sikkerhetsstrategi og oversikt over systemene som behandler personopplysninger er ikke gjennomgått jevnlig siden utarbeidelsen for seks år siden. Det viste seg også at beskrivelsen av sikkerhetsorganisasjonen ikke var oppdatert og viste til organisatoriske funksjoner som i dag ikke eksisterer i kommunen. Videre er det ikke gjennomført noen overordnet risikovurdering av informasjonssikkerhet siden 2000. Kommunen har et sikkerhetsreglement, men dette er ikke oppdatert på 12 år. Generelt syntes heller ikke sikkerhetsreglement og sikkerhetsdokumentasjonen å være vidt kjent blant de revisjonen var i kontakt med. Fysisk sikring av serverrom og backup av kommunes data synes å være tilfredsstillende.

Undersøkelsen har avdekket mangler i forhold til anbefalinger i God IT-skikk når det gjelder IT-drift. Revisjonen har funnet at IT-strategien 2002-2005 ikke var fornyet. Det forelå ikke beredskapsplaner for sikring av IT-driftskontinuitet ved alvorlige hendelser. Videre fant revisjonen at det ved endringshåndtering ofte ble gjennomført endringer direkte ut mot brukerne uten at det var testet i lukket miljø først. Noe som kan innebære en risiko for driftskontinuiteten. Det viste seg også at dokumentering av endringer innen IT ikke ble foretatt jevnlig. Gjennomgangen av arbeidsdelingen innen IT i kommunen viste at denne oppfattes å være tilfredsstillende ved at en skilte mellom styringsrollen, bestillerrollen og leverandørrollen i kommunen.

2 Innledning

2.1 Bakgrunn for prosjekt

Revisjonen skal i følge kommuneloven § 78 pkt. 2 og forskrift om revisjon § 6 og § 7 utføre forvaltningsrevisjon. Dette innebærer tilsyn med at den økonomiske forvaltning foregår i samsvar med gjeldende bestemmelser og vedtak, og foreta en systematisk vurdering av bruk og forvaltning av de kommunale midler med utgangspunkt i oppgaver, ressursbruk og oppnådde resultater.

I kontrollutvalgsmøte 1. desember 2005, saksnummer 23/05, ble det vedtatt prioritering mellom forvaltningsrevisjonsprosjekter basert på plan for forvaltningsrevisjon for perioden 2006-2008. *IKT* ble vurdert å være et prioritert område for forvaltningsrevisjon for 2006. Bakgrunnen for valg av prosjekt var overordnet analyse for forvaltningsrevisjon som vurderte risikoen innen IT - sikkerhet og ytelse til å være høy. I kontrollutvalgsmøte 31.8.2006 ble det vedtatt gjennomført forvaltningsrevisjonsprosjekt *Informasjonssikkerhet og IT-drift* i Oppegård kommune.

3 Formål og problemstillinger

3.1 Formål

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

3.2 Problemstillinger

Revisjonen har valgt følgende problemstillinger:

- **Informasjonssikkerhet**
  - Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?

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

3.3 Avgrensninger

Prosjektet omfatter ikke en kartlegging av Oppegård 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 avgrenses til et overordnet nivå i kommunen, og inkluderer av den grunn ikke de enkelte virksomheters/ansattes aktiviteter.

4 Metoder og gjennomføring

Undersøkelsesopplegget er basert på en kombinasjon av analyser av utlevert dokumenter og intervjuer med personer i ulike roller knyttet til IKT og informasjonssikkerhet i kommunen. Dokumentene analyseres for å vurdere om de er tilstrekkelige i forhold til aktuelle anbefalinger (beste praksis) knyttet til IT-drift og krav i forskrift knyttet til informasjons-sikkerhet. Intervjuene av ansatte og ledere innen IKT og informasjonssikkerhet skal gi en forståelse av praksis og etterlevelsen av regelverket og rutiner i kommunen.

4.1 Gjennomføring

Prosjektet er gjennomført i perioden september – desember 2006 av rådgiver Ole Anders Sandtrøen. Revisjonens kontaktperson i Oppegård kommune var kommunens IKT-sjef.

Revisjonen valgte ut følgende roller for intervju:

- Kommunens IKT-sjef
- Kommunens sikkerhetsansvarlig
- 3 systemansvarlige for systemer som behandler sensitive personopplysninger
- 1 IT-kontaktperson for en skole
- 2 ansatte ved IKT-avdelingen

For dokumentgjennomgangen ble kontaktpersonen i Oppegård kommune forespurt om de dokumentene de hadde innen informasjonssikkerhet og IT-drift, samt kommunens IT-strategi. I tillegg har revisjonen innhentet noen dokumenter. Tabell 1 viser oversikt over hvilken dokumentasjon som er gjennomgått av revisjonen.

Tabell 1 Liste over revisjonens dokumentunderlag fra Oppegård kommune

Tittel	Dato
Sikkerhetsmål	18.10.00
Sikkerhetsstrategi	02.05.00
Oversikt over personopplysninger som kommunen behandler	18.10.00
Referat fra ledelsens siste gjennomgang av sikkerhetsmål, strategi og organisering	14.09.00
Sikkerhetsreglement for Oppegård kommunes EDB-virksomhet	14.04.94
Informasjon om ansvars- og myndighetsforhold (sikkerhetsorganisasjon)	14.06.00
Rapport fra sist utførte risikoanalyse	20.06.00
Rapportering av sikkerhetsbrudd (avvikshåndtering)	14.06.00
Rutiner for bruk av E-post	22.01.01
Kriseplan for Oppegård kommune	Okt. 05
IT-strategi 2002-2005	Sep. 01
Administrativt delegasjonsreglement for Oppegård kommune	16.02.06
Rutinebeskrivelse for å ta servere og SAN ned og opp	18.05.06
Backuprobot: Oversikt over tiltak ved en del vanlige feilmeldinger	ingen dato
Rutine for bytte av backuptaper	28.05.04
Oversikt over ansatte i IKT-avdelingen i Oppegård kommune	ingen dato
Oversikt over systemer (IT) i Oppegård kommune	ingen dato
Rollebeskrivelse: Systemforvalter for fagsystem ”MARTHE” (nå Familia)	22.06.04
Årsrapporter for Oppegård kommune, 2003,2004 og 2005	
Budsjett og økonomiplan for årene, 2004, 2005, 2006 og 2007	

4.2 Dataenes pålitelighet og gyldighet

Undersøkelsen bygger i første rekke på opplysninger fra gjennomgang av dokumenter og intervjuer med ulike personer som har sentrale roller i forhold til informasjonssikkerhet og IT-drift. Informasjon som er fremkommet er referert og bekreftet av de som er intervjuet.

Kvalitetssikring av datagrunnlaget omfatter en vurdering av pålitelighet (reliabilitet) og gyldighet (validitet). Pålitelighet er et uttrykk for hvor nøyaktig innsamling av data har vært, og at det ikke er skjedd systematiske feil underveis i innsamlingen. Revisjonen har sett på dokumenter knyttet til informasjonssikkerhet og IT-drift. Alle dokumenter som er gjennomgått er mottatt fra kommunen og i tillegg bekreftet å være gjeldende dokumentasjon. Intervjuene med ansatte har også båret preg av refleksjon og åpenhet.

Gyldighet brukes gjerne som et uttrykk for om vi har målt det vi ønsker å måle. Gyldigheten ble sikret ved at revisjonen innhentet sentrale dokumenter som er spesifisert i revisjons-kriteriene og intervjuet ansatte om praktiseringen av rutiner definert i revisjonskriteriene og i kommunens egne dokumenter.

5 Informasjonssikkerhet

5.1 Revisjonskriterier

I personopplysningsloven (POL) § 13 pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Dette omfatter å sørge for at tilstrekkelig sikkerhetsfaglig kompetanse er tilgjengelig hos den behandlingsansvarlige. Virksomhetens behandlingsansvarlige er normalt representert ved den administrative ledelse. For en kommune vil dette normalt være ved rådmann.

I tillegg til ansvar for sikkerheten i egen organisasjon, må den behandlingsansvarlige også forsikre seg om at informasjonssikkerheten er tilfredsstillende hos kommunikasjonspartnere og leverandører. 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.

Personopplysningsforskriften (POF) definerer nærmere hvilke krav som hviler på kommunen for at tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger finner sted. Revisjonen har valgt å vektlegge følgende krav i denne undersøkelsen:

Personopplysningsforskriften § 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.

Personopplysningsforskriften § 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.

Personopplysningsforskriften § 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.

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

Personopplysningsforskriften § 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 (rådmann). 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. For mindre virksomheter kan det likevel være nødvendig å legge begge funksjoner til en og samme person. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

Personopplysningsforskriften § 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, 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.

5.2 Faktabeskrivelse

5.2.1 Sikkerhetsmål, strategi og oversikt over personopplysninger kommunen behandler

Oppegård kommune leverte i oktober 2000 *"søknad til Datatilsynet om godkjenning av informasjonssikkerhet i forbindelse med at sensitive personopplysninger skal behandles i dedikert informasjonssystem"*. Dokumentet går under fellesbetegnelsen internkontroll-håndbok og inneholder de gjeldende versjoner av dokumentene på området. Tabellen under viser en oversikt over kommunens sikkerhetsmål, sikkerhetsstrategi og oversikt over behandling av personopplysninger i kommunen. Den viser også dato for utarbeidelse, godkjenning og godkjenningsinstans og hvilke forskriftshjemler i personopplysnings-forskriften de hører inn under. I tillegg viser den kommunens EDB-sikkerhetsreglement

Tabell 2 Oversikt over dokumenter på området

Tittel på dokument	Utarbeidet dato	Revidert/ Godkjent	Godkjennings-instans	Krav lov/forskr.
Sikkerhetsmål	18.10.00	14.09.00	Rådmannen	POF. § 2-3, 2. ledd
Sikkerhetsstrategi	02.05.00	20.09.00	Rådmannen	POF. § 2-3, 3. ledd
Oversikt over personopplysninger som kommunen behandler	18.10.00	Ikke datert	Rådmannen	POF. § 2-4
Referat fra ledelsens siste gjennomgang av sikkerhetsmål, strategi og organisering	14.09.00	18.10.00	Rådmannen	POF. § 2-3, 4. og 5. ledd
Sikkerhetsreglement for Oppegård kommunes EDB-virksomhet	Ikke dato	14.04.94	Adm. utvalget	

Sikkerhetsmål og sikkerhetsstrategi ble i sin tid godkjent av Datatilsynet, revisjonen vurderer derfor ikke innholdet av disse dokumentene. I tillegg til disse overordnede dokumentene skal ledelsen ha en jevnlig gjennomgang av sikkerhetsmål, sikkerhetsstrategi, oversikt over personopplysninger som behandles og sikkerhetsorganisasjon. Tabellen over viser at siste gjennomgang av dette ble gjennomført i forbindelse med søknaden til Datatilsynet i 2000. Dokumentene viser også til systemer og organisatoriske funksjoner som er endret siden 2000.

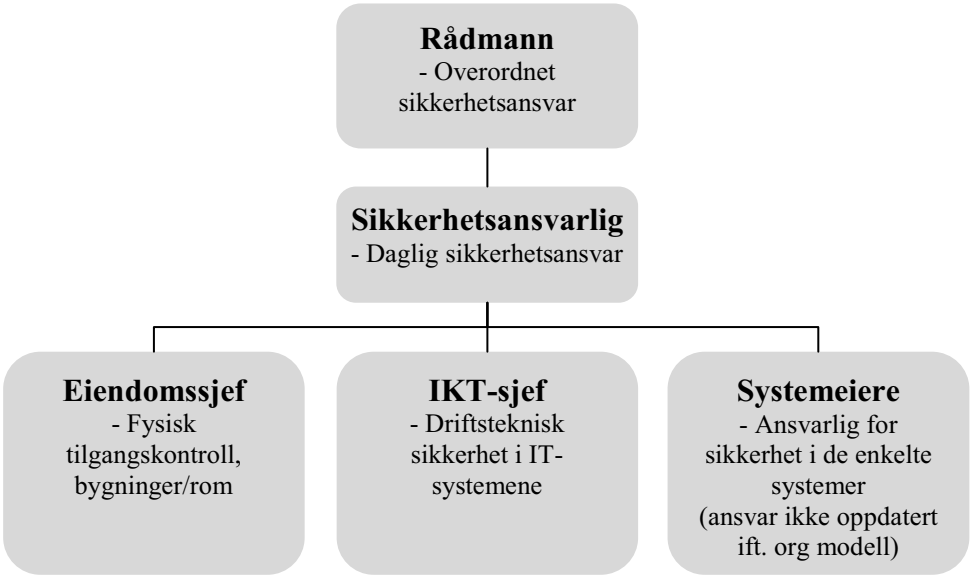
EDB-sikkerhetsreglementet ble utarbeidet i 1994. Den behandler blant annet ikke nyere trusler knyttet til Internett, bruk av mobile enheter, e-post og lignende. På kommunens intranettsider er det derimot oppgitt særskilte rutiner for bruk av e-post, men på intranettsidene er ikke EDB-sikkerhetsreglementet nevnt. I samtale med revisjonen oppgir tidligere IKT-sjef at det arbeides med å oppdatere sikkerhetsreglementet for kommunen.

5.2.2 Sikkerhetsorganisasjon

Tabell 3 Oversikt over dokumenter knyttet til sikkerhetsorganisasjon

Tittel på dokument	Utarbeidet dato	Revidert/ Godkjent	Godkjennings-instans	Krav lov/forskr.
Informasjon om ansvars- og myndighetsforhold (sikkerhetsorganisasjon)	14.06.00	20.09.00	Rådmannen	POF. § 2-7

Kommunens beskrivelse av sikkerhetsorganisasjonen er fra 20.9.2000 og refererer til roller som i dag har falt bort som følge av kommunens tonivåmodell. Oversikten under viser hoveddelene i sikkerhetsorganisasjonen i Oppegård kommune slik den fremstår for revisjonen i dag. Rådmannen har det overordnede ansvaret for informasjonssikkerheten i kommunen. Det daglige sikkerhetsansvaret er plassert hos en sikkerhetsansvarlig. De øvrige rollene definerer hvilke personer som har ansvar for ulike deler av sikkerhetsarbeidet i kommunen.



Figur 1 Organisasjonskart – sikkerhetsorganisasjonen i Oppegård kommune (revisjonens tolkning)

Sikkerhetsansvarlig oppgir til revisjonen at det ikke har vært tid nok til å prioritere å oppdatere beskrivelsen av sikkerhetsorganisasjonen. Dette området oppfattes ikke så presserende som andre lov- og forskriftskrav til kommunen. På spørsmål om sikkerhetsansvarlig har nok tid til dette arbeidet oppgir sikkerhetsansvarlig at det ikke er avsatt en bestemt andel tid til denne oppgaven. Sikkerhetsansvarlig oppgir videre at en baserer seg på at sikkerheten i det daglige fungerer.

Sikkerhetsansvarlig opplever at han i det daglige har mest kontakt med virksomhetene og IKT-sjef, og mindre med rådmannen. Det er hovedsakelig i situasjoner hvor noe går galt at

rådmann er involvert, da hovedsakelig på driftssiden. Sikkerhetsansvarlig oppgir at rådmann baserer seg på at disse oppgavene ivaretas av andre og blir kun involvert hvis det er et problem av ett eller annet slag.

5.2.3 Sikkerhetsrevisjon, risikoanalyse, avvikshåndtering og oppdateringer

Tabell 4 Oversikt over dokumenter knyttet til risikoanalyse og avvikshåndtering

Tittel på dokument	Utarbeidet dato	Revidert/ Godkjent	Godkjennings-instans	Krav lov/forskr.
Rapport fra sist utførte risikoanalyse	08.10.99 20.06.00	20.09.00	Rådmannen	POF. § 2-4
Rapportering av sikkerhetsbrudd (avvikshåndtering)	14.06.00	Ikke datert	Rådmannen	POF. § 2-6

Sikkerhetsrevisjon

I revisjonens gjennomgang av sikkerhetsrevisjonsarbeidet kom det fram at det ikke er gjennomført sikkerhetsrevisjoner. I intervju med revisjonen bekrefter sikkerhetsansvarlig at det ikke har vært gjennomført en overordnet og dokumentert sikkerhetsrevisjon i Oppegård kommune siden 2002 da vedkommende fikk oppgaven som sikkerhetsansvarlig.

Risikoanalyse

Risikoanalyse ble sist gjennomført i 2000 og er en oppdatering av KPMG sin risikoanalyse fra 1999. Etter dette er det ikke gjennomført noen overordnet risikoanalyse knyttet til informasjonssikkerhet i kommunen. I følge sikkerhetsansvarlig i kommunen er risikovurderingen som ble gjort i 2000 fremdeles gyldig. Sikkerhetsansvarlig oppgir også at det ved spesielle hendelser og endringer gjennomføres konkrete risikovurderinger for disse.

Avvikshåndtering

Internkontrollhåndboken har et eget avsnitt for avvikshåndtering ”Rapportering av sikkerhetsbrudd”. Rutinen i kommunen er at avvik skal rapporters på eget skjema vedlagt internkontrollhåndboken. Avviksrapporten leveres enten den person i sikkerhetsorganisasjonen som har myndighet til å behandle sikkerhetsbrudd eller sikkerhetsansvarlig dersom dette anses som nødvendig i saken.

Sikkerhetsansvarlig oppgir at det aldri er blitt meldt inn noen avvik vedrørende informasjonssikkerhet siden vedkommende startet som sikkerhetsansvarlig i 2002. Sikkerhetsansvarlig oppgir videre at disse normalt skal sendes inn til ham. Det eneste som har kommet inn av avvik knyttet til IT har vært av driftsmessig karakter, slik som arbeidsmiljø og mangelfulle systemer. Det har vært ett tilfelle hvor noen prøvde å trenge inn i IT-systemene (hacking). I forbindelse med den hendelsen ble det avholdt et møte hvor det ble vurdert at sikringssystemene fungerte.

På spørsmål om hvordan ansatte i kommunen var kjent med sikkerhetsorganisasjonen og sikkerhetsreglementet, oppgir sikkerhetsansvarlig at de ansatte får opplæring i konfidensialitetstenkningen av de systemansvarlige. Det er ikke noe felles kurs hvor informasjonssikkerhet inngår. EDB-sikkerhetsreglementet skal i følge sikkerhetsansvarlig være tilgjengelig ute i virksomhetene sammen med andre styringsdokumenter. Revisjonen spurte noen systemansvarlige om de var kjent med sikkerhetsorganisasjon og EDB-sikkerhetsreglementet, men ingen av de revisjonen var i kontakt med var kjent med

disse. På spørsmål om de viste hvem sikkerhetsansvarlig var, svarte kun én av tre systemansvarlige at de var kjent med hvem dette var.

Sikkerhetsansvarlig oppgir selv at det er en utfordring i kommunen å få informasjon ut til medarbeiderne. Mange har ikke tilgang til kommunens intranett som ligger på en Lotus Notes løsning. Disse er avhengige av at all informasjon distribueres skriftlig av virksomhetslederne, noe som skjer i varierende grad fra virksomhet til virksomhet.

5.2.4 Fysisk sikring

All elektronisk informasjon i kommunens datasystemer som behandler sensitiv personopplysninger og helseregisteropplysninger, behandles i et lukket system og lagres i kommunens serverpark.

Den fysiske sikringen av sensitiv personopplysninger i elektronisk form begrenser seg hovedsakelig til serverrommet i kommunen. Revisjonen befarte serverlokalet til kommunen sammen med IKT-sjef. Serverrommet er sikret på følgende måte:

- Bygningsmessig plassert midt i bygget uten direkte adgang via yttervegger
- Smekklås og sikkerhetslås tilknyttet alarmsentral med rutiner ved hendelser. Det vurderes å innføre adgangskort med kode, i forbindelse med utskifting av låser på rådhuset, for ytterligere å styrke sikkerheten.
- Branndør og Argon brannslukkingssystem
- Aircondition/kjøling
- Hevet gulv for kabling og beskyttelse mot oversvømmelse/vannlekkasje
- Nødstrømsaggregat som automatisk slår inn ved strømbrudd og UPS (batteristrøm) for å sikre strømtilførsel inntill aggregatet overtar eller systemet er tatt ned på betryggende måte (slått av)

I tillegg til fysisk sikring av serverrom er backup av informasjonen som lagres der viktig. I Oppegård kommune har man følgende backuprutine:

- Backup tas inkrementelt. Det vil si at det tas backup av alle filer som er endret siden siste fullstendige backup. Backupen tas på tape som står i rack i samme rom som serverparken står. Backuptaper som er ferdig tas ut og legges i egen brannsikker safe som er plassert i rådhusets bomberom.

IKT-sjef opplyser at backuprutinene er under revidering for ytterligere sikring av kommunens data. Et tidligere utskiftet disklagringssystem er planlagt brukt til å foreta backup. Dagens tapelagringssystem er planlagt plassert i eget bygg, fortrinnsvis Kolben kulturhus.

5.3 Vurdering

Revisjonen har undersøkt Oppegård kommunes etterlevelse av kravene til sikkerhetsmål, sikkerhetsstrategi og hvilken oversikt som foreligger for personopplysninger som behandles i kommunens informasjonssystemer. Undersøkelsen viser at Oppegård kommune har etablert sikkerhetsmål, sikkerhetsstrategi og oversikt over personopplysninger som kommunen behandler. Sikkerhetsbestemmelsene stiller videre krav om at ledelsen gjennomgår disse dokumentene jevnlig. I Oppegård kommune ble siste gjennomgang av sikkerhetsmål,

sikkerhetsstrategi og sikkerhetsorganisering gjennomgått den 14.9.2000. Ingen av de nevnte dokumentene har blitt oppdatert siden 2000.

Kommunens sikkerhetsreglement er fra 1994 og behandler blant annet ikke hvordan kommunens medarbeidere skal forholde seg til nyere trusler. Et gammelt sikkerhetsreglement som mangler oppdatert informasjon har betydning for reglementets aktualitet blant de ansatte i kommunen. Dette kan igjen få betydning for informasjonssikkerhet ved at bestemmelsene i reglementet ikke følges.

Beskrivelsen av sikkerhetsorganisasjonen i Oppegård kommune er ikke oppdatert siden 2000 og er på enkelte områder misvisende, ved at det vises til organisatoriske funksjoner som har falt bort som følge av omorganiseringen av kommunen. Sikkerhetsorganisasjonen, slik den fremstår for revisjonen i dag (figur 1.), viser at rollen som sikkerhetsleder og driftsleder er klart definert. I tillegg er rollene lagt til forskjellige medarbeidere i kommunen. Dette skillet mellom utøvende og kontrollerende funksjon er i tråd med anbefalt praksis fra Datatilsynet.

Sikkerhetsrevisjon er en aktivitet som skal gjennomføres i alle deler av virksomheten innen en 12 måneders periode. Resultatene fra dette skal også dokumenteres. I Oppegård kommune viser det seg at sikkerhetsansvarlig aldri har gjennomført sikkerhetsrevisjon siden vedkommende fikk oppgaven i 2002. Revisjonen har heller ingen informasjon som tyder på at det er gjennomført sikkerhetsrevisjon siden forskriften trådde i kraft 1.1.2001. Sikkerhetsrevisjon er en viktig kontrollaktivitet for å sørge for at nødvendig informasjonssikkerhet ivaretas i kommunen. Uten denne kontrollaktiviteten vil det være vesentlig risiko for at manglende informasjonssikkerhet oppstår og ikke blir fanget opp og korrigert.

Risikoanalyse ble sist gjennomført i 2000. Risikoanalysen er i følge sikkerhetsansvarlig fremdeles gyldig. Revisjonen oppfatter det som viktig at det gjennomføres risikoanalyser jevnlig, spesielt i forbindelse med endringer innen IT for å påse at risikovurderingene er gyldige.

I Oppegård kommune er det etablert en avvikshåndteringsrutine i internkontrollhåndboken av 2000. Sikkerhetsansvarlig oppgir at det aldri har vært rapportert avvik. At det aldri har vært rapportert inn avvik fra rutiner og sikkerhetsbrudd kan tyde på at avvik enten rapporters på annen måte eller at rutiner for avvikshåndtering ikke er kjent blant medarbeiderne i kommunen. Oppegård kommune har ikke inkludert informasjonssikkerhet som en del av grunnopplæringen innen IT, og de systemansvarlige revisjonen var i kontakt med var lite kjent med sikkerhetsarbeidet i kommunen. Dette kan tyde på at informasjon om informasjonssikkerhet ikke er tilstrekkelig kommunisert til medarbeiderne og systemansvarlige i kommunen.

Den fysiske sikringen av serverrom er gjennomgått. Det er gjort flere tiltak for å sikre dette mot ulike fysiske risikofaktorer som uautorisert adgang, brann, høy temperatur, strømbrudd og oversvømmelse. Etter revisjonens oppfatning synes de fysiske sikringstiltakene å være tilfredsstillende.

IKT-avdelingen har etablert faste backuprutiner og tapene fra backup oppbevares innlåst i brannsafe i rådhusets bomberom. Dette synes å være en god løsning ved oppbevaring i samme bygg som selve serverrommet. Revisjonen har fått opplyst at IKT-avdelingen vurderer å endre

på backuprutinene slik at det også foretas en backup i et annet bygg enn det serverne står i. Revisjonen oppfatter dette som et positivt tiltak i forhold til å trygge dataene til kommunen.

6 IT-drift

6.1 Revisjonskriterier

Overordnede mål, retningslinjer og rutiner
COBIT[1] og God IT-skikk *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: [2]

- **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.

Arbeidsdeling
Statskonsult[3] og KS[4] *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:

- **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.

[1] Control Objectives for Information and Related Technology (COBIT) er utviklet av Information Systems Audit and Control Association (ISACA) og IT Governance Institute (ITGI) og gir anbefalinger for god IT-skikk.
[2] Anbefaling til God IT-skikk (nr. 1) Dokumentasjon av IT-systemer 2001
[3] IKT i det offentlige 2002
[4] Verktøykasse for IKT-planlegging 2004 Analyse av IKT organiseringen, Kommunenes Sentralforbund TN 7

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.

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.

6.2 Faktabeskrivelse

6.2.1 Overordnede mål og strategier

Oppegård kommunes IT-strategi gjelder for perioden 2002-2005 og var sist revidert i september 2001. IT-strategien beskriver Oppegård kommunes målsetninger for IT.

"Strategiens overordnede mål er å bidra til å sikre at informasjonsteknologi tas i bruk som et optimalt strategisk virkemiddel for å effektivisere tjenesteproduksjonen og yte god service til innbyggerne."

Strategien har fire hovedmål hvor IT skal bidra til:

1. *Økt lokaldemokrati og lokal identitet*
2. *Effektivisering og serviceorientering av kommunens tjenesteproduksjon*
3. *Utvikling av en effektiv og attraktiv organisasjon*
4. *Kompetanseutvikling og læring i organisasjonen*

IT-strategien beskriver at alle IT-prosjekter skal godkjennes av et IT-råd som skal sikre at alle prosjekter skjer innen en helhet. Mandatet beskrives på følgende måte:

"IT-rådet skal være et støtteorgan for rådmannens ledergruppe ved å koordinere og foreslå prioriteringer av kommunens IT-strategi ut i fra en helhetsvurdering av hva som tjener kommuneorganisasjonen best."

Det konkretiseres videre en prosedyre for gjennomføring av IT-prosjekter hvor det stilles krav til kostnadsbeskrivelse, gevinster, behov under prosjekt og lignende. Det er IT-sjef og avdelingsleder som avgjør om anskaffelsen/endringen organiseres som et IT-prosjekt.

IKT-sjef oppgir at IT-rådet ikke har vært i funksjon så lenge han har vært i stillingen. Tidligere IT-sjef oppgir også at IT-rådet ikke har vært i funksjon. IKT-sjef oppgir at dette trolig skyldes at de største endringene knyttet til IT ble gjennomført rundt den tiden IT-strategien for 2002-2005 ble etablert. Siden de viktige strategiske veivalgene for hvilken

programplattform kommunen skulle ha var avgjort, var det ikke behov for et IT-råd som møtte regelmessig.

En gjennomgang av investeringsplanene for Oppegård kommune for perioden 2004-2006 viser følgende oppføringer:

Tabell 5: Oversikt over IT investeringer i investeringsprogrammet i perioden 2004-2006

Beskrivelse	Utgifter
INVESTERINGSPROGRAM 2004	
IKT-avdelingen: Oppgradering av operativsystem på server - klient med mer.	3 500 000
VA: Driftsovervåkningssystem, målepunkter	200 000
Høykom: Oppegård kommunes bidrag til bredbåndnett	1 056 000
Pleie- og omsorg, håndterminaler til IT-system anskaffet i 2001	500 000
INVESTERINGSPROGRAM 2005	
IKT-avdelingen: Utskifting eldre utstyr, oppgraderinger av nett med mer	2 300 000
VA: Driftsovervåkningssystem, målepunkter og oppgradering programvare	200 000
IKT Follo: flere delprosjekter knyttet til samarbeidet	650 000
Byggesak og geodata: Digitalt byggesaksarkiv, midler til avslutning prosjekt	520 000
INVESTERINGSPROGRAM 2006	
IKT-avdelingen: fornyelse av IT-utstyr	1 300 000
IKT-avdelingen: Bredbånd og IP-telefoni i Oppegård kommune	2 500 000
VA: Driftsovervåkningssystem, målepunkter	200 000

Av denne framkommer det ingen nye IT-investeringer som er av en slik størrelse at de inkluderes i investeringsprogrammet. IKT Follo er den eneste posten som ut i fra investeringsprogrammet betyr at det igangsettes IT-prosjekter. Disse prosjektene er derimot interkommunale prosjekter. Fra 1.1.2007 går IKT Follo over i en driftsfase og Oppegård kommune arbeider med en fornyet IT-strategi, planlagt ferdigstilt i løpet av våren 2007, hvor det interkommunale samarbeidet innen IT er planlagt inkludert.

6.2.2 Arbeidsdeling og organisering av IKT-avdelingen

Oppegård kommune er organisert etter en tonivåmodell hvor ledelsen består av rådmannen og fire kommunalsjefer og 50 selvstendige virksomheter. IKT-funksjonen ligger under Stab/støtte funksjoner. Organisasjonskartet (figur 2, neste side) viser en oversikt over de ulike funksjonene knyttet til IKT i kommunen.

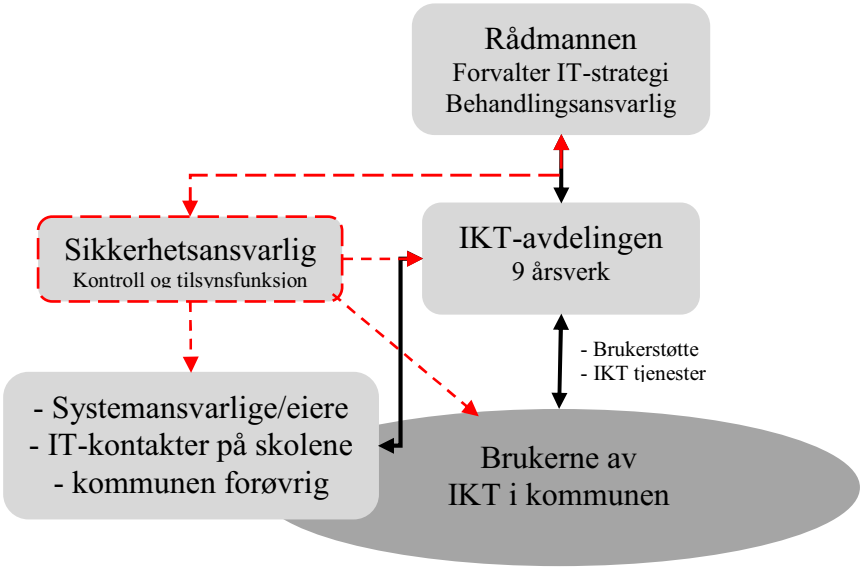
Rådmannen har det overordnede ansvaret for IKT i kommunen. Rådmannens ledergruppe behandler strategisk viktige spørsmål knyttet til IKT-satsninger og forvalter IT-strategien til kommunen. Rådmannen som øverste administrative leder er også behandlingsansvarlig for informasjonssikkerheten i kommunen iht. personopplysningsloven §13.

Sikkerhetsansvarlig har den daglige kontroll og tilsynsfunksjonen for informasjons-sikkerheten i kommunen. Denne rollen er plassert utenfor IKT-avdelingen.

Systemansvarlige/eierne har ansvaret for sine respektive fagsystemer og skal fungere som bindeledd mellom virksomhetene og IKT-avdelingen. De administrerer tilganger, tilrettelegger/tilpasser fagsystemene, ivaretar opplæring og brukerstøtte, melder inn behov for oppdateringer til IKT-avdelingen og ivaretar sikkerhet.

IT-kontakter i skolene har ansvaret for drift av maskinparken for elever og lærere på den enkelte skole, administrerer tilganger til brukerkonto/e-post. De øvrige maskinene som rektor, administrativt ansatte og lignende bruker er driftet av IKT-avdelingen direkte. Maskinparken

for elever og lærere er i ferd med å bli oppgradert til samme plattform som kommunen for øvrig. Dette skal lette arbeidet for IKT-avdelingen og IT-kontaktene. IT-kontaktene er personell ved skolene som får fristilt timeressurser til IT-kontaktoppgaver. Det er opp til den enkelte rektor å vurdere hvilket behov eller økonomisk ramme det er for denne oppgaven, derfor kan timetallet til IT-kontaktene variere fra skole til skole.



Figur 2 Organisasjonskart over ulike IT-relaterte funksjoner i Oppegård kommune (revisjonens utgave)

IKT-avdelingen er organisert under Stab/støttefunksjoner og er delegert overordnet operativt ansvar for drift av IKT i kommunen. Arbeidsfeltet er å tilby IKT-tjenester til kommunen hvor det er ca 780 brukere i administrativt nett og ca 2500 brukere i elevnettet. Den økonomiske rammen for IT i kommunen er på ca 11 millioner kr i driftsbudsjett og ca 1,5 millioner kr i investeringsbudsjett.

Avdelingen består av ni årsverk fordelt på to grupper:

- administrativ gruppe består av IKT-sjef og to ansatte, hvorav den ene har ansvar for opplæring/kursvirksomhet/anskaffelser og den andre administrerer personalforhold og noen IT-oppgaver.
- Driftsgruppen består av de øvrige seks ansatte som jobber med IT-driftsoppgaver.

Det er noen funksjoner som går på rundgang mellom medarbeiderne. Helpdesk-funksjonen (brukerstøtte) følger en åtte dagers rullering. Alle ansatte har en dag hver på helpdesk fra 08:00 til 15:30. Den som har ansvar for helpdesk mottar henvendelser fra brukerne via telefon, voicemail og e-post. Innkomne henvendelser blir logget og enten løst av helpdesk eller videreformidlet til det øvrige driftspersonellet. I tillegg til brukerstøtte overvåker den som har helpdesken serverpark via et overvåkningssystem. De ansatte har også en uke hver med ansvar for backup og en uke hver med gjennomgang av e-post som er stoppet av kommunens brannmur[5]. IKT- sjef oppgir at brukerstøtte er en utfordrende oppgave som det jobbes med å forbedre. Det er blant annet anskaffet nytt brukerstøttesystem som skal brukes i 2007 som vil kunne hjelpe dette arbeidet. Dette systemet skal være webbasert hvor blant annet de som melder inn saker vil kunne se status for saken.

[5] Brannmur er en logisk innretning for å hindre uautorisert eller uønsket kommunikasjon mellom deler av et datanettverk

Gjennomgang av den formelle kompetansen i IKT-avdelingen viser at seks av ni ansatte har utdannelse på høgskolenivå. Av disse er det to med utdannelse innen IT, to med ingeniørutdannelse og to med annen teknologisk utdannelse. De øvrige tre ansatte har mer variert bakgrunn på videregående nivå, lang arbeidserfaring og sertifiserte IT-kurs.

IKT-sjef oppgir at IKT-avdelingen har en flat struktur. Det er fokus på at kunnskapen i organisasjonen forvaltes slik at alle oppgaver skal kunne ivaretas av flere ansatte. Dette for å redusere sårbarheten ved eventuelt fravær av kritisk personell, som for eksempel ved ferieavvikling eller sykdom. Det satses også på å styrke kompetansen på sentrale områder for IKT-avdelingen som nettverk/printere, e-post og database/applikasjon. Det skal være minst to ansatte som har dybdekompetanse innen disse områdene. IKT-sjef oppgir at alle har fått en stillingsinstruks i forbindelse med ansettelse i sin tid. Det er derimot ikke utarbeidet nye i forbindelse med omlegging av rutinene i IKT-avdelingen.

IKT-sjefen oppgir at avdelingen har hatt en svært utfordrende tid, spesielt i forbindelse med systemkrasjen i februar 2006. Avdelingen har høyt sykefravær som medfører økt arbeidsbelastning for de ansatte. Dette fører også til at fokuset i større grad har vært rettet mot løpende driftsoppgaver og mindre på utviklingsoppgaver, dokumentering og lignende. Tabellen under viser utviklingen i sykefravær for første og andre tertial 2006. Denne viser at sykefraværet er høyt i IT-avdelingen i 1. tertial, men på nivå med kommunen for øvrig. 2. tertial viser at sykefraværet økte ytterligere i IT-avdelingen, mens kommunen for øvrig hadde langt lavere sykefravær.

Tabell 6 Sykefraværet i IKT-avdelingen for 1 og 2 tertial 2006

Enhet / kvartal	2006 1. tertial	2006 2. tertial
Sykefravær IKT-avdelingen	9,67 %	11,27 %
Sykefravær Stab og støtte (inkl IT)	10,21 %	7,87 %
Sykefravær Oppegård kommune	10,50 %	8,87 %

6.2.3 Driftskontinuitet

Beredskapsplanlegging

IT-driftsområdet har ikke egen beredskapsplan som omhandler beredskapstiltak knyttet til IT-relaterte katastrofer/alvorlige hendelser. IKT-sjef oppgir at det jobbes med å utarbeide en beredskapsplan for IT.

Måling og evaluering av kontinuitet

I Oppegård kommune er det etablert et styringssystem basert på balansert målstyring. I årsrapportene for 2003 til 2005 oppgis oppetid som en styringsindikator for Stab og støtte (tabell 7). Målingen baserer seg på hvilken oppetid det er i tidsrommet 08:00 til 15:30 fratrukket planlagt nedetid.

Tabell 7 Oppetiden for IT i Oppegård kommune 2003-2005[6]

År	Ønsket tilstand (08:00-15:30)	Godt nok	Måling (08:00-15:30)	Antall timer pr år
2005	(99 %)	(95 %)	☺	
2004	99 %	95 %	99,8 %	3,9
2003	100 %	95 %	99 %	19,5

[6] Oppegård kommune gikk i 2005 bort fra å angi tall i rapporteringen, og over til kun bruk av smilefjes.

Målingen gjelder hele nettverket eller kritiske servere/applikasjoner. Prosentnivået for "Godt nok" skal i følge IKT-sjef gjelde ved 24/7 drift, men dette framkommer ikke av årsrapportene. IKT-sjef oppgir at de ikke logger driftsforstyrrelser, men at de har anskaffet et overvåkningssystem (Microsoft Operation Manager) for serverne som også logger driftsavbrudd. På sikt skal denne også fungere for nettverket i kommunen.

Ved planlagt nedetid gis det informasjon til brukerne enten via intranettløsningen til kommunen under OK-nytt eller ved direkte oppslag hvor intranettet ikke er tilgjengelig, som for eksempel på skolene.

6.2.4 Endringshåndtering og dokumentering

Endringshåndtering

IKT-sjef oppgir at det ikke er fastlagte rutiner vedrørende endringshåndtering. Ved endringer foretas endringene enten med direkte test ut mot brukerne, eller mot en testbase hvis dette er tilgjengelig. Endringene foretas derfor i hovedsak "live" mot brukerne.

Endringer/oppdateringer av fagsystemer meldes som regel inn til IKT-avdelingen av de systemansvarlige som får beskjed om oppdateringer fra leverandørene. Systemansvarlige autoriserer endringene, mens IKT-avdelingen står for den tekniske tilretteleggingen. To av tre systemansvarlige som revisjonen var i kontakt med opplevde at IKT-avdelingen til tider var forsinket og gav lite informasjon om når endringene/oppdateringene var foretatt. Den som var tilfreds med IKT-avdelingen gav uttrykk for at vedkommende ikke oppdaterte fagprogrammet så ofte som det var anledning til, blant annet for å unngå å belaste IKT-avdelingen unødig. Endringer/oppdateringer av betydning for fellessystemer/IT-utstyr ligger inn under IKT-avdelingen ansvar og autoriseres av IKT-sjef.

Dokumentering skjer i etterkant av endringer hvor det legges inn informasjon om endringer som er foretatt. Det brukes en felles database for endringer som igjen blir lagt inn som dokumentasjon. Det brukes også en endringslogg hvor løpende endringer legges inn. IKT-sjef oppgir videre at en ikke har vært flinke nok til å følge dette opp. Sykdom og andre presserende oppgaver gjør at avdelingen har større fokus på andre oppgaver. IKT-sjef oppgir at han har satt fokus på at de ansatte skal dokumentere endringer jevnlig.

Dokumentasjon

Dokumentasjonen knyttet til IT er fordelt i tre hovedtyper som beskrevet i revisjonskriteriene.

- **Systemdokumentasjon** beskrives i Oppegård kommune gjennom den dokumentasjonen som leverandørene leverer sammen med løsningene. Siden Oppegård kommune ikke utvikler programvaren selv utvikler de i liten grad systemdokumentasjon.

- **Driftsdokumentasjon** utarbeides løpende i en felles database for IKT-avdelingen. Her finnes informasjon og prosedyrer for de forskjellige systemene for å sikre at drift av disse lettes.

- **Brukerdokumentasjon** er også en type dokumentasjon som i hovedsak leverandørene for IT-utstyr/applikasjonene leverer sammen med løsningene. I intervju med

systemansvarlige oppgis det at denne dokumentasjonen tilpasses de rutinene som innarbeides internt i kommunen slik at den endelige brukerdokumentasjonen er oppdatert og riktig for kommunen.

6.3 Vurdering

Revisjonen har undersøkt om Oppegård kommune har etablert IT-strategi og at denne er forankret i kommunens mål og planer. Oppegård kommune etablerte en IT-strategi i 2001 som gjaldt for perioden 2002-2005. IT-strategien var forankret i kommunens mål og planer slik God IT-skikk anbefaler. IT-strategien gjaldt kun fram til 2005 og det er ikke kommet noen oppdatering av denne. Innholdsmessig er beskrivelsen av IT-rådets rolle sentral. Dette rådet har ikke vært i funksjon de siste årene. En viktig funksjon ved IT-rådet var å påse at IT-prosjekter var tilstrekkelig kvalitetssikret med henhold til blant annet nytte/kost vurderinger. Dette er en funksjon som i IT-rådets fravær ikke klart defineres i kommunen. Siden IT-strategien ikke har blitt oppdatert har det i realiteten ikke vært en dokumentert strategisk forankring for de valgene som er gjort innen IT fra 2005. Revisjonen oppfatter det som nødvendig å ha en IT-strategi som er forankret i kommunens mål og planer, og som indikerer hvilken strategisk satsning kommunen har på IT og hvordan denne skal nås. Revisjonen registrerer at det skal etableres ny IT-strategi i 2007.

Revisjonen har undersøkt organisering og arbeidsdeling av IT i Oppegård kommune. Faktabeskrivelsen viser at IKT-avdelingen er sentralt plassert i organisasjonen med kort vei til rådmann. Videre har systemansvarlige/systemeierne en selvstendig rolle som ansvarlige for sine fagapplikasjoner. Disse driftes av IKT-avdelingen som er leverandør av IT-driftstjenester. Arbeidsdelingen følger i hovedsak skillet mellom styringsrollen (rådmannen), bestillerrollen (systemansvarlige/eiere) og leverandørrollen (IKT-avdelingen). Denne rollefordelingen synes å være i tråd med anbefalt arbeidsdeling for IT.

IKT-avdelingen er organisert slik at det er kunnskapsmessig overlapp for viktige funksjoner. Dette kan bidra til redusert sårbarhet ved uforutsett fravær hvor en ikke er avhengig av at enkeltpersoner er tilgjengelig. Kompetansemessig har IKT-avdelingen en stor andel ansatte med høyskoleutdannelse innen IT/teknologiske fag, i tillegg vektlegges kursing av de ansatte. Dette er positivt for å sikre at nødvendig kompetanse er tilstede i kommunen for å løse IT-oppgavene. Revisjonen registrerer at sykefraværet er høyt i IKT-avdelingen. Høyt sykefravær kan få stor innvirkning på oppgaveutførselen og over tid kan et stort press på øvrig personell også føre til ytterligere sykefravær.

Kontinuitet i driften er sentralt for en effektiv utnyttelse av IT som verktøy i oppgaveutførelsen i kommunen. God IT-skikk anbefaler at en etablerer beredskapsplaner for hvordan en ivaretar driftskontinuiteten ved alvorlige hendelser. IKT-avdelingen har ikke etablert en beredskapsplan hvor rutiner for håndtering av alvorlige hendelser tas opp. Dette er et viktig verktøy for å sikre at en er forberedt for alvorlige hendelser og kan redusere konsekvensene ved disse. Revisjonen registrerer at det er igangsatt et arbeid med å få etablert en beredskapsplan.

Logging av driftsforstyrrelser er viktig. Ofte kan mindre forstyrrelser over tid belaste virksomheten mest. Et annet viktig aspekt er at det gis informasjon og tilbakemelding til systemeiere og brukere ved driftsavbrudd. Revisjonens undersøkelse viser at driftsforstyrrelser ikke logges i Oppegård kommune. IKT-avdelingen er derimot i gang med å etablere et system for overvåkning og logging av serverpark. I tillegg etableres det et nytt

helpdesksystem som skal lette arbeidet med å registrere og behandle feil i IT-systemene. Det opplyses også at brukere og systemeiere varsles ved planlagte driftsbrudd. Revisjonen ser positivt på at IKT-avdelingen jobber for å få på plass et system for logging av driftsbrudd. Dette vil kunne bidra til at en får raskt oversikt over hvilke problemer som oppstår og hva som ble gjort for å løse disse.

Revisjonen registrerer videre at en i Oppegård kommune praktiserer måling av oppetid som en indikator for god IT-drift. Oppetiden i Oppegård kommune har gått tilbake fra 2004 til 2005. Driftsbruddet i 2006 indikerer at det for dette året også er en oppetid som er lavere enn ønsket.

IKT-avdelingen har ingen fastlagt rutine for endringshåndtering. Ved endringer foretas disse ofte direkte mot brukerne. I tilfeller hvor det er tilgjengelig testbaser foretas tester først. Dette er en praksis som kan innebære en risiko for driftskontinuiteten i tilfeller hvor brukerne tar i bruk systemer etter endringer som ikke i tilstrekkelig grad er testet og risikovurdert på forhånd. Planlagte endringer foretas som oftest ved at de som har ansvaret for systemet melder inn endringen til IKT-avdelingen som foretar endringene. Dette er en praksis som er i tråd med god IT-skikk ved at den sikrer at de som har ansvaret for systemene også autoriserer endringene. Dokumentasjonen skjer i etterkant av endringene i en felles database for IKT-avdelingen. Denne loggingen av endringer er ikke blitt fulgt opp i den grad som er ønskelig. Dokumentasjon er en viktig aktivitet for å kunne spore mulige feilkilder, sikre at en har oversikt over hvilke versjoner og endringer som er gjort.

Revisjonen har gjennomgått dokumentasjonsrutinene i kommunen med sikte på å få en oversikt over hvordan systemdokumentasjon, driftsdokumentasjon og brukerdokumentasjon håndteres i kommunen. Siden kommunen kjøper IT-programmer fra leverandører i stedet for å utvikle dette selv, er systemdokumentasjon og brukerdokumentasjon i hovedsak dokumentert av leverandørene. Brukerdokumentasjonen oppgis å bli supplert av systemansvarlige på de områdene hvor det gjøres tilpasninger til kommunens rutiner. Revisjonene oppfatter dette som en tilfredsstillende praksis i lys av at kommunen kjøper systemene. Driftsdokumentasjon føres løpende i en database som er tilgjengelig for ansatte i IKT-avdelingen. Denne formen for dokumentering synes også å være tilfredsstillende.

7 Konklusjon

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard. Konklusjonene i rapporten er delt opp i områdene informasjonssikkerhet og IT-drift.

7.1 Informasjonssikkerhet

- Sikkerhetsrevisjon er ikke gjennomført i Oppegård kommune de siste seks årene slik personopplysningsforskriften krever.

- Sikkerhetsmålene, sikkerhetsstrategien og oversikten over systemer som behandler personopplysninger er etablert iht. forskriftskravene. Disse er derimot ikke gjennomgått jevnlig siden utarbeidelsen for seks år siden.

- Beskrivelsen av sikkerhetsorganisasjonen er ikke oppdatert siden utarbeidelsen for seks år siden og refererer til roller som i dag ikke eksisterer i Oppegård kommune.

- Overordnet risikovurdering av informasjonssikkerheten er ikke gjennomført siden 2000.

- EDB-sikkerhetsreglementet for Oppegård kommune er ikke oppdatert på 12 år.

- Sikkerhetsreglementet og øvrig sikkerhetsdokumentasjon synes ikke å være vidt kjent i kommunen.

- De fysiske sikringstiltakene av serverrom og backup av data oppfattes å være tilfredsstillende.

7.2 IT-drift

- IT- strategien 2002-2005 er ikke fornyet.

- Beredskapsplaner for sikring av IT-driftskontinuitet ved alvorlige hendelser foreligger ikke.

- Endringer av IT-systemene gjennomføres ofte direkte ut mot brukerne. Dette kan innebære en risiko for driftskontinuiteten.

- Dokumentering av endringer innen IT foretas ikke jevnlig.

- Arbeidsdelingen innen IKT i kommunen oppfattes å være tilfredsstillende.

8 Anbefalinger

8.1 Informasjonssikkerhet

Revisjonen mener Oppegård kommune må gjennomføre tiltak som sikrer at informasjonssikkerhetsarbeidet gjennomføres i tråd med regelverket, herunder:

- At kommunen igangsetter sikkerhetsrevisjon i kommunen som dekker hele virksomheten innen en 12 måneders periode. Resultatet av sikkerhetsrevisjonen må også dokumenteres.

- At ledelsen jevnlig gjennomgår sikkerhetsdokumentasjon for å sikre at den til enhver tid er oppdatert. Dette kan gjerne gjøres sammen med gjennomgang av resultatene fra den årlige sikkerhetsrevisjonen av kommunen.

- At en reviderer de overordnede risikovurderingene fra 2000, for å påse at de fremdeles er gyldige for kommunen.

Videre vil revisjonen anbefale Oppegård kommune å:

- Gjøre informasjonssikkerhetsbestemmelsene i kommunen bedre kjent blant de ansatte.

- EDB-sikkerhetsreglementet bør oppdateres og sammenhengen mellom sikkerhetsreglementet og de øvrige dokumentene innen informasjonssikkerhet bør avklares.

- Sikre serverrom ytterligere ved å gjennomføre de planlagte forbedringene av adgangsbegrensingen ved å benytte adgangskort med kode.

8.2 IT-drift

Revisjonen mener Oppegård kommune kan gjennomføre tiltak som forbedrer IT-drift, herunder:

- Etablere ny IT-strategi som dokumenterer de strategiske føringene for utviklingen av kommunens IT-satsning.

- Etablere beredskapsplan med rutiner for håndtering av uønskede IT-relaterte hendelser som har alvorlige eller katastrofale konsekvenser for virksomheten.

- I størst mulig grad unngå å teste direkte i produksjonssystemene ved planlagte endringer, for å sikre at det ikke oppstår utilsiktede konsekvenser for driftskontinuiteten.

24 JAN. 2007

Follo Distriktsrevisjon
Postboks 3010

1402 SKI

Vår ref.:	Deres ref.:	Ark.:	Dato:
Saksbeh.: EHA	J.nr 10/7	064	23.01.2007
Saksnr.: 06/2253-4			

SVAR - FORVALTNINGSREVISJON IT-SIKKERHET OG DRIFT

Rådmannens høringsuttalelse

Nedenstående uttalelse er i hovedsak disponert etter den "Guide til høringsuttalelse fra rådmannen" som Distriktsrevisjonen oversendte sammen med rapporten.

Har informasjon om prosjektets mål vært tilstrekkelig klar?
Vi har forstått det slik at foranledningen til kontrollutvalgets vedtak den 31.08.06 var den alvorlige driftsstansen Oppgård kommune hadde i sine IT-systemer sommeren 2006 og at utvalget ønsket å kartlegge at det var tatt skritt til at dette ikke skal gjenta seg. Videre har vi oppfattet det slik at revisjonen samtidig ønsket å revidere kommunens systemer for informasjonssikkerhet mer generelt.

Metode
I forhold til valgt metode, anvendte kilder og data, har vi ingen kommentar.

Revisjonskriterier
I forhold til revisjonskriteriene på "informasjonssikkerhet" har vi intet å bemerke. I forhold til kriteriene innen "IT-drift"har vi merket oss at revisjonen bruker COBIT og God-IT skikk som referanse. Dette er en innfallsvinkel som da bygger på et gitt sett med parametere. Oppegård kommune bruker NS7799 og NS-ISO 1799 som grunnlag for utarbeidelse av sin informsjonssikkerhet. Selv om disse avviker noe, antar vi at det ikke har vesentlig betydning for resultatet.

Samlet vurdering av rapportens konklusjoner.
Rapporten peker på flere mangler i dokumentasjonen på sikkerhetssiden i tilknytning til Oppegård kommunes informasjonssystem. I all hovedsak har påpekte mangler tilknytning til at kommunens internkontrollsystem ikke er gjennomgått, fornyet og dokumentert på flere år slik at tilfredsstillende dokumentasjonen på IT-sikkerhet foreligger. Rådmannen erkjenner at dette er kritikkverdig og har, som redegjort for i punktet nedenfor, nedsatt en arbeidsgruppe

for å revidere sikkerhetsystemene, fornye rutiner og lage en plan for implementering. I løpet av de nærmeste måneder vil et revidert sikkerhetsregime være på plass.
En finner imidlertid grunn til å understreke at hovedproblemet ikke er at sikkerhetssystemer ikke er etablert, men at de ikke er fulgt tilfredsstillende opp, dokumentert etter organisasjonsendringer, ny teknologi og programvare er tatt i bruk etc.

I forhold til rapportens anbefaling om sikring av kommunens serverrom, har vi merket oss at Distriktsrevisjonen i utgangspunktet anser den fysiske sikringen som tilfredsstillende. En ytterligere forsterkning av denne sikkerheten vil bli vurdert i sammenheng med en mer gjennomgående vurdering av fysisk sikkerhet og adgangskontroll i hele rådhuset.
Rapporten gir viktige informasjon og forsterker behovet for prioritere IKT-sikkerhetsarbeidet både ved å oppdatere og vedlikeholde gode systemer.

Planlagte tiltak for på IT-området.

Kommunen har en vedtatt IKT-plan (2002 – 2005) som angir mål, retningslinjer og prioriteringer for dette området. Planen er i det vesentlige fulgt opp, og det vil med det første bli etablert et prosjekt for å fornye denne. Når dette ikke har skjedd tidligere må dette bl.a. ses i sammenheng med:
IKT-Follo
Oppegård kommune har siden 2002 inngått i et interkommunalt samarbeid med 5 andre Follokommuner og utviklet følgende IKT-tjenester: Felles brukerportal, Felles kart- og geodatasystemer, Bredbånd mellom rådhusene i Follo, en Folloportal samt en felles system for dokumenthåndtering(NOARK 4) Arbeidet har vært et pilotprosjekt som er gjort med vesentlig finansiell støtte fra staten/Høykom, og har bidratt til regionen er i front når det gjelder muligheter for virtuell kommunikasjon med innbyggerne og næringsliv. Prosjektet vil i løpet av 1. kvartal 2007 fremlegge en strategi for fremtidig IKT-samarbeid i Follo.

IKT i oppegårdskolen.
Rådmannen har etablert et prosjekt for hvordan IKT bør anvendes og utvikles i Oppegårdskolen. Prosjektet er en oppfølging av Kvalitetsutviklingsplanen for oppegårdsskolen og skal angi hvordan den nasjonale satsingen på digitale verktøy skal kunne realiseres lokalt.

Bredbånd til alle kommunale virksomheter.
Over de siste årene har Oppegård kommune arbeidet systematisk med å fremføre bredbånd til alle kommunale virksomheter. Målsettingen er å sikre tilfredsstillende kapasitet på kommunikasjonslinjene mellom de ulike enhetene og til rådhuset. Arbeidet ventes i det vesentlige avsluttet i løpet av 2007. Da vil de aller fleste lokasjoner være tilknyttet samme nett slik at kapasitetsbegrensningene på tidligere linjer kan elimineres.

Sikkerhetsprosjekt.
På ettersommeren 2006 ble det etablert en arbeidsgruppe med ansvar for å revidere gjeldene IKT-sikkerhetsplan og fornye rutiner og systemer for implementering av disse.

Helhetlig IKT-plan for Oppegård.
Som nevnt har gjeldende IKT-plan for kommunen utgått på dato. Innholdsmessig har imidlertid vedtatt plan vært relevant inntil nylig. I løpet av 2. kvartal er siktemålet å etablere et prosjekt som kan arbeide frem en helhetlig IKT-strategi for kommunen. Dette arbeidet har vi ventet med noe tid både av kapasitetsmessige grunner, men også fordi en har ansett

det som hensiktsmessig å få frem resultater fra omtalte delprosjekter før en fornyer denne mer overordnede og helhetlige planen.

Ovennevnte viser at kommunen har iverksatt en rekke tiltak og prosjekter for å oppgradere og fornye kommunes IKT – funksjon. Etter alvorlige driftsforstyrrelsene i 2006 er det allerede tatt skritt for å forhindre nye alvorlige hendelser bl.a. ved at nødstrømsforsyning er på plass, lagringskapasitet er utvidet og gamle servere er faset ut etc. Den arbeidsgruppe for sikkerhetsoppdatering som er etablert vil ventelig avgi sin rapport i med det første. De anførsler og anbefalinger som fremkommer i revisjonens rapport forutsatt fulgt gjennom dette arbeidet slik at kommunen igjen kan få på plass et helhetlig og betryggende sikkerhetsopplegg for sin IKT-funksjon.

Fremdrift.
I omtalen av pågående prosjekter er det redegjort for fremdriftene av disse. Når det gjelder sikkerhetsopplegget vil et revidert sikkerhetsregime bli implementert så snart forslagene fra den omtalte arbeidsgruppen foreligger, slik at alt kan være på plass i løpet våren. Deretter vil det bli etablert systemer for løpende oppfølging. Når det gjelder en ny overordnet IKT-plan anses det realistisk at forslag vil kunne foreligge ved utgangen av inneværende år.

Sluttbemerkninger.
Revisjonens gjennomgang av kommunens sikkerhetssystemer innenfor IKT har avdekket at både systemer og rutiner er utilstrekkelige ved at de ikke har blitt kritisk gjennomgått, revidert og fornyet på flere år. Revisjonens anførsler og forslag vil bli fulgt opp i det arbeidet som er på gang for oppdatere og fornye sikkerhetssystemene. I ettertid er det ikke vanskelig å erkjenne at oppgradering, fornyelse og dokumentasjon av kommunens IT-sikkerhetsopplegg burde hatt større oppmerksomhet de siste årene. Fokus har i for stor grad vært konsentrert om å identifisere nye anvendelsesområder for teknologien. Ikke minst IKT-Follo prosjektet og bredbåndsprosjektet har krevd mye oppmerksomhet og ressurser. En helhetlig gjennomgang av sikkerhetsopplegget ble påbegynt i høst og et betryggende opplegg planlegges å være på plass i løpet av de nærmeste måneder.

Kolbotn 23.01.01

Harald Toft
Rådmann

Leif Nateid
IKT-sjef

Espen Hallan
Spesialkonsulent

10 Revisjonens kommentarer til rådmannens uttalelse

Revisjonen ser positivt på at rådmannen i sin uttalelse har sluttet seg til de konklusjoner og anbefalinger som revisjonen har fremmet i rapporten. Revisjonen ser det også som positivt at rådmannen gjennomfører en helhetlig gjennomgang av sikkerhetsopplegget slik at dette er på plass i løpet av de nærmeste måneder. Revisjonen har for øvrig merket seg at rådmannen opplever at rapporten gir viktig informasjon og forsterker behovet for å prioritere IKT-sikkerhetsarbeidet i kommunen.

11 Litteraturliste

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

Forskrift om behandling av personopplysninger (personopplysningsforskriften) 1.1.2001.

Lov om behandling av personopplysninger (personopplysningsloven) 1.1.2001

Statskonsult: IKT i det offentlige 2002

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