FORVALTNINGSREVISJON

IKT

Kvalitetskrav og informasjonssikkerhet

SØMNA KOMMUNE

22.11.2017

KomRev Trøndelag IKS

FORORD

KomRev Trøndelag IKS har gjennomført denne forvaltningsrevisjonen på oppdrag fra kontrollutvalget i Sømna kommune. Prosjektet er gjennomført i perioden februar til oktober 2017.

Kontrollutvalget skal påse at forvaltningsrevisjon gjennomføres, jf. lov om kommuner og fylkeskommuner (kommuneloven) § 77 nr 4. Forvaltningsrevisjon innebærer å gjøre systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger[1].

Undersøkelsen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001.

Revisjonsteamet har bestått av prosjektleder Unni Romstad, prosjektmedarbeidere Rikke Haave og Margrete Haugum og kvalitetssikrer Marte Bjørnelv.

Revisor har vurdert egen uavhengighet overfor Sømna kommune, jfr. kommuneloven § 79 og § 6. Vi kjenner ikke til forhold som er egnet til å svekke tilliten til vår uavhengighet og objektivitet.

Vi takker alle som har bidratt med informasjon i prosjektet.

En oversikt over tidligere gjennomførte prosjekter fra KomRev Trøndelag IKS finner du på vår hjemmeside www.krt.no/

Steinkjer 22.11.2017

Unni Romstad

Unni Romstad
Oppdragsansvarlig forvaltningsrevisor

[1] Forskrift om revisjon i kommuner og fylkeskommuner mv (revisjonsforskriften) § 7

INNHOLDSFORTEGNELSE

1. Innledning 7
1.1 Bestilling 7
1.2 Bakgrunn 7
1.3 Problemstillinger 7
1.4 Revisjonskriterier 8
1.5 Metodisk tilnærming og gjennomføring 8
Intervju 8
Spørreundersøkelse 8
Dokumentgjennomgang 9
Samlet vurdering av datagrunnlag og metode 9
Avgrensning 9
2. Sømna kommune og IT-avtaler 10
2.1 Tidligere vertskommuneløsning med Brønnøy kommune 10
2.2 Avtale med Evry Norge AS fra 2014 10
2.3 Avtale med IT Partner Helgeland 12
2.4 Oppsummering av avtaler 14
3. Planlegging og organisering 15
3.1 Revisjonskriterier 15
3.2 Data 15
3.2.1 IT-strategi 15
3.2.2 Myndighet og ansvar 16
Formell organisering 16
Roller og ansvarsfordeling IKT 17
3.2.3 Informasjonsarkitektur 18
3.2.4 Risikostyring 19
3.3 Vurdering 19
IT-strategi 19
Myndighet og ansvar 20
Informasjonsarkitektur 20
Risikostyring 21
4. Anskaffelser og implementering 22

4.1 Revisjonskriterier 22
4.2 Data 22
4.2.1 Kravspesifikasjon 22
4.2.2 Anskaffelse og vedlikehold av teknologisk infrastruktur 22
4.2.3 Anskaffelse og vedlikehold av programmer og applikasjoner 23
4.2.4 Installasjon og godkjenning av systemer 23
4.3 Vurdering 24
Kravspesifikasjon 24
Plan for anskaffelse og vedlikehold av maskinvare 24
Plan for anskaffelse og vedlikehold av programvare 24
Installasjon og godkjenning av systemer 24
5. Driftsleveranse og støtte 25
5.1 Revisjonskriterier 25
5.2 Data 25
5.2.1 Servicenivå 25
5.2.2 Brukeropplæring 26
5.2.3 Uønskede hendelser og problemer 27
5.2.4 Håndtering av data 28
5.2.5 Fysiske omgivelser 28
5.3 Vurdering 29
Servicenivå 29
Brukeropplæring 29
Uønskede hendelser og problemer 30
Håndtering av data 30
Fysiske omgivelser 30
6. Kontrolltiltak 31
6.1 Revisjonskriterier 31
6.2 Data 31
6.2.1 Internkontroll 31
6.2.2 Sikring av konfidensialitet 32
6.2.3 Sikring av integritet 33
6.2.4 Sikring av tilgjengelighet (sikring mot tap av data) 34
6.3 Vurdering 34

Internkontroll 34
Konfidensialitet 35
Integritet 35
Tilgjengelighet 36
7. Konklusjon 37
Hovedkonklusjon 38
8. Anbefalinger 39
9. Rådmannens kommentarer 40
9.1 Høringssvar 40

Liste over figurer

Figur 2.1: Oversikt over avtaler og innhold 14

SAMMENDRAG

I forbindelse med overordnet analyse og Plan for forvaltningsrevisjon ble IKT avdekket som et risikoområde i Sømna kommune. Det ble pekt på at kommunen ikke har den IKT-teknologien den trenger, og at systemet er sårbart. Fra enkelte enheter ble det uttrykt bekymring for sikkerheten i systemet.

Problemstillingen handler om *i hvor stor grad har Sømna kommune sikret et godt styringssystem for IT gjennom å ivareta utvalgte styrings- og kontrollmål i anerkjent kvalitetsstandard (COBIT).*

Vi ser på de fire hovedområdene i kvalitetsstandarden:

- Planlegging og organisering
- Anskaffelser og implementering
- Driftsleveranse og støtte
- Kontrolltiltak

Revisjonskriteriene er utledet av kvalitetsstandarden samt personopplysningsloven med tilhørende forskrifter og E-forvaltningsforskriften.

Rapporten bygger på informasjon innhentet gjennom intervju med rådmann og IT-tekniker, spørreundersøkelse til ansatte i Sømna kommune og dokumentgjennomgang.

Sømna kommune har avtale med Serit IT Partner Helgeland om drift av egen serverpark og brukerstøtte. Kommunen har også en ASP-avtale (programvare tilgjengelig via nett og ekstern lagring av data) med Evry om økonomisystemet Agresso, saks- og arkivsystemet ephorte og epostsystem, hvor Evry har ansvar for drift og lagring av data. Kommunen har en egen IT-tekniker og en lærling innenfor IKT.

Rapporten er en gjennomgang av hvordan Sømna kommune har løst oppgavene på IKT-området sammenholdt med de kravene som stilles i kvalitetsstandarden COBIT. Undersøkelsene viser at Sømna kommune mangler en IKT-strategi med mål og handlingsplaner, herunder en sikkerhetsstrategi. Kommunen er i gang med å utarbeide en digitaliseringsstrategi og i forbindelse med organisasjonsgjennomgangen høsten 2017 skal det på plass en digitaliseringsansvarlig i stab. Kommunen har en utdatert ROS-analyse for IKT området fra 2013 som inneholder den systematikken som Cobit etterspør. Ansvar- og myndighet er noe uklart innad i kommunen, mens ansvarsforholdet til IT Partner er klargjort gjennom avtalen med IT Partner. Gjennom samarbeidet med IT Partner har kommunen fått en god informasjonsarkitektur som er dokumentert.

Det forelå ingen kravspesifikasjon ved inngåelsen av avtalen med IT Partner. Kommunen har heller ingen planer for anskaffelse og vedlikehold av maskinvare og

programvare. IT Partner bistår kommunen med installasjon og godkjenning av systemer og dette er ivaretatt på en god måte.
Kommunens IKT-systemer fungerer bra og brukerne er fornøyd med servicen. Det er noe uklart for brukerne at IT-tekniker er førstelinje for brukerstøtte og noen henvendelser går direkte til IT Partner sin brukerstøtte. Brukerne gis opplæring i bruk av systemet, programmer og sikkerhet, men denne er noe mangelfull spesielt på sikkerhet. Brukernes tilganger til systemet følger av tilganger som gis i AD (Active directory) og uønskede hendelser loggføres. Kommunen har god fysisk sikring på eget utstyr og fjernlagring er godt sikret.

Kommunen har ikke internkontroll på plass på IKT-området, men arbeidet med sikkerhetsnorm er startet opp. Sensitive data ligger på egne områder og tilgangen styres gjennom AD (Active directory), men det er mulig at gruppetilganger gjøre at flere enn nødvendig har tilgang på noen områder. Kommunen har i samarbeid med IT Partner gode backup rutiner som sikrer at data er tilgjengelig.

På bakgrunn av disse vurderingene, konkluderer revisor med at Sømna kommune delvis har sikret et godt styringssystem for IT/IKT gjennom at utvalgte styrings- og kontrollmål i anerkjent kvalitetsstandard (COBIT) er ivaretatt.

På bakgrunn av vurderinger og konklusjon vil revisor anbefale:

- Kommunen bør sikre at digitaliseringsstrategi inneholder det som forventes av en IKT-strategi som viser overordnede mål og veivalg samt konkrete handlingsplaner, herunder en sikkerhetsnorm/strategi og en plan for investering og utskifting av maskinvare.
- Kommunen bør tydeliggjøre og dokumentere ansvar og myndighet innenfor IKT-området og herunder etablere rutiner for hvem som skal ta tilgang til hva.
- Kommunen bør utarbeid en internkontroll på IKT-området.
- Kommunen bør oppdatere ROS-analysen.

1. INNLEDNING

1.1 Bestilling

På bakgrunn av Plan for forvaltningsrevisjon 2012-2015[2] har kontrollutvalget i Sømna kommune bestilt en forvaltningsrevisjon med tema IKT (informasjons- og kommunikasjonsteknologi). I rapporten brukes hovedsakelig begrepet IKT, mens IT (informasjonsteknologi) brukes synonymt, eksempelvis i stillingstittel.

Kontrollutvalget behandlet skisse til prosjektplan for prosjektet i sitt møte 13.02.17 /sak 02/2017. Endelig prosjektplan ble vedtatt 13.2.2017. Fokus i prosjektet er på planlegging og organisering, anskaffelser og implementering, driftsleveranse og støtte og kontrolltiltak.

1.2 Bakgrunn

I forbindelse med overordnet analyse og Plan for forvaltningsrevisjon ble IKT avdekket som et risikoområde i Sømna kommune. Det ble pekt på at kommunen ikke har den IKT-teknologien den trenger, og at systemet er sårbart. Fra enkelte enheter ble det uttrykt bekymring for sikkerheten i systemet.

IKT-teknologi skal være et virkemiddel for virksomheten og skal bidra til at man når de vedtatte målsettingene. For at kvalitet i IKT skal være tilfredsstillende, må kvalitetskrav for ivaretakelse av informasjonssikkerhet være oppfylt. Dette gjelder både planlegging og organisering, anskaffelse og implementering, driftsleveranse og støtte samt kontrolltiltak (internkontroll).

1.3 Problemstillinger

Revisor har endret ordlyden i problemstillingen noe i forhold til vedtatt prosjektplan. Dette har ingen betydning for hva som er undersøkt.

Følgende problemstilling er besvart i undersøkelsen:

I hvor stor grad har Sømna kommune sikret et godt styringssystem for IT gjennom å ivareta utvalgte styrings- og kontrollmål i anerkjent kvalitetsstandard (COBIT)?

Vi ser på de fire hovedområdene i kvalitetsstandarden:

- Planlegging og organisering
- Anskaffelser og implementering
- Driftsleveranse og støtte
- Kontrolltiltak

[2] Vedtatt i kontrollutvalget 14.11.16/sak 15/2016 og i kommunestyret 20.12.16/sak 97/16

I tillegg gir vi en kort presentasjon av den inngåtte avtalen mellom Sømna kommune og IT Partner Helgeland AS, leverandør av tjenester knyttet til IT-løsninger som maskinvare, infrastruktur og programvare. Sømna har også et samarbeid med Brønnøy kommune som beskrives nærmere.

1.4 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot.

I dette prosjektet er kriteriene hentet fra:

- COBIT (Control objectives for Information and Related Technology) Kvalitetsstandard for IKT
- Personopplysningsloven med tilhørende forskrifter
- E-forvaltningsforskriften

Revisjonskriteriene er utledet i vedlegg 1, samt følger punktvis under de enkelte problemstillingene.

1.5 Metodisk tilnærming og gjennomføring

Prosjektet er gjennomført i perioden februar til oktober 2017. Rapporten bygger på informasjon innhentet gjennom intervju, spørreundersøkelse og dokumentgjennomgang. Intervju er benyttet for å få innsikt i hvordan kommunen arbeider på IKT-området og spørreundersøkelsen er benyttet for å innhente informasjon fra brukerne av IKT-systemet.

Intervju

I forbindelse med prosjektet har vi intervjuet rådmann og IT-tekniker i Sømna kommune. Intervjuet ble gjennomført etter en intervjuguide, og det ble lagt opp til en gjennomgang av tema og hovedspørsmål. Informantene fikk på forhånd tilsendt stikkord for samtalen. Referat fra intervjuet er verifisert av informantene i etterkant for å rette opp eventuelle faktafeil og misforståelser.

Senere i prosjektgjennomføringen ble IT-teknikeren stilt noen oppfølgingsspørsmål på telefon samtidig med at flere kommunale dokumenter ble etterspurt. På dette tidspunktet ble også IT Partner stilt noen oppklaringsspørsmål på telefon i forhold til avtalen med kommunen og det arbeidet de gjør for kommunen, for å få bedre innsikt i IT Partner sin rolle.

Spørreundersøkelse

En spørreundersøkelse ble distribuert til alle ansatte i Sømna kommune som bruker IKT til daglig i sin jobb. Det ble sendt ut en nettbasert spørreundersøkelse til ansatte i

kommunen som har egen epostadresse og som bruker IKT-systemet. Kommunen fikk oversendt en papirutgave av spørreskjemaet slik at spørreskjemaet kunne distribueres til brukere av IKT-systemet, som ikke har egen epostadresse. Vi fikk ingen papirbaserte skjema i retur.

Spørreundersøkelsen ble sendt til 133 personer, hvorav 62 svarte. Dette ga en total svarprosent på 46,6 prosent. Av disse 62 er det 54 personer som oppgir at de bruker kommunens IKT-system i jobben.

Undersøkelsen kartlegger kjennskap til avtaler med leverandører av IKT-tjenester, IT-strategier og ROS-analyser (spesielt rettet mot ledernivået), videre kjennskap til ansvars– og myndighetsforhold for bruk av informasjonssystemet, systemets tilgjengelighet, forhold omkring brukerstøtte og opplæring. Det er også spurt om rutiner for sikring av dataenes konfidensialitet og integritet, og sikring mot tap av data.

Dokumentgjennomgang

Referanselista viser hvilke skriftlige dokumenter vi har brukt som kilder. Den består av følgende litteratur:

- Litteratur om informasjonssikkerhet
- Litteratur om personopplysninger

Videre har vi gjennomgått relevante dokumenter som Sømna kommune har utarbeidet, samt avtaler og relevante dokumenter fra Brønnøy kommune knyttet til samarbeidet innenfor IKT.

Samlet vurdering av datagrunnlag og metode

Vi mener det har vært tilstrekkelig å intervjue rådmann og IT-teknikeren i kombinasjon med spørreundersøkelse til ansatte i kommunen og en dokumentgjennomgang. I spørreundersøkelsen kan det for noen spørsmål være litt uklart hva som ligger til grunn for respondentenes svar. Dette er kommentert i presentasjonen av dataene. Oppfølgingsspørsmål til IT-teknikeren og oppklaringsspørsmål til IT Partner har bidratt til å utfylle bildet fra intervjuet og dokumenter ytterligere. Informasjonen vi har samlet gjennom ulike metoder peker i samme retning.

Vår samlede vurdering er at metodebruk og kildetilfang i dette prosjektet gir et tilstrekkelig grunnlag til å svare på problemstillingene.

Avgrensning

Prosjektet har ikke sett på forhold som berører problemstillinger omkring kommunens eventuelle plikt til å melde/søke konsesjon for behandling av personopplysninger.

2. SØMNA KOMMUNE OG IT-AVTALER

Sømna kommune har avtale med Serit IT Partner Helgeland AS (heretter kalt IT Partner) om driftsteknisk støtte. Videre har kommunen en avtale med Brønnøy kommune om en ASP-løsning[3] for sak- og arkivsystem, epost og økonomisystem. Kommunen har også en avtale med Evry Norge AS (heretter kalt Evry) om kommunikasjonsløsningen til ASP. I tillegg finnes det avtaler med ulike programvareleverandører med kostnader knyttet til lisenser og oppdateringer.

2.1 Tidligere vertskommuneløsning med Brønnøy kommune

I 2010 ble det etablert et interkommunalt samarbeid på IKT-området mellom kommunene Brønnøy, Sømna, Vevelstad, Vega og Bindal. Samarbeidsavtalen ble fornyet 5.9. 2014 med en videreføring av ASP-programvare for saks- og arkivprogrammet ephorte og økonomisystemet Agresso, samtidig ble avtalen utvidet til å omfatte ASP-drift av disse systemene og ASP-drift av kommunens epost og intranettløsning med virkning fra 2015. Brønnøy kommune er vertskommune for samarbeidet, og hadde fram til 2014 stått for drift, vedlikehold og brukerstøtte for løsningen. Avtalen som ble inngått omfattet også de øvrige kommunene, men det ble for disse kommunenes vedkommende tatt forbehold om politisk behandling. Dersom disse kommunene ønsket å tiltre avtalen måtte det skje innen 31. oktober 2014. Alternativt ville tjenesteleveransen fra Brønnøy kommune opphøre 31. desember 2014.

Den nye avtalen inneholdt følgende elementer:

- Ny gruppevareløsning
- Ny løsning for e-post, kalender og kontakter ble innført
- Oppgradering og utvikling av sak- og arkivsystem
- Etablering av intranett
- Ekstern drift og vedlikehold
- Opplæring

Sømna kommune vedtok å ikke tiltre den nye avtalen. Revisor har etterspurt sakspapirer i forbindelse med at kommunestyret besluttet ikke å fortsette samarbeidet med Brønnøy. Vi har pr dato ikke mottatt disse.

2.2 Avtale med Evry Norge AS fra 2014

Høsten 2014 startet Brønnøy kommune prosessen med utlysing av leveranse av både applikasjoner og drift, og 6. februar 2015 inngikk Brønnøy kommune en totalavtale med Evry, som inkluderte en fornyelse av avtalen avtale med Evry fra 5. september

[3] ASP-løsning (Active Server Pages) innebærer at programmer og dokumenter ligger på eksterne servere som driftes og vedlikeholdes av Evry, men at det oppleves som å jobbe lokalt på egen pc.

2014. Tidlig i 2015 fikk Sømna (sammen med de øvrige Sør-Helgelands-kommunene) tilbud om å tiltre totalavtalen mellom Brønnøy kommune og Evry. Denne nye avtalen erstattet alle tidligere avtaler med Evry og samlet alle leveransene til kommunene på Sør-Helgeland i én avtale.

Merkostnaden for Sømna kommunens vedkommende ble i saksframlegget anslått til ca. 120 000 kroner året til drift, mens investeringene ble anslått til ca. 880 000 kroner.

Sømna besluttet *ikke* å tre inn i den nye avtalen med Evry. Avtalen fra 5. september 2014 om Agresso, ephorte og epostsystem ble stående. Sømna kommune konkluderte som Bindal, mens kommunestyrene i Vega kommune og Vevelstad kommune vedtok å tiltre avtalen fra 2015.

Sømna kommune ble da stående tilbake med ASP-avtalen som Brønnøy kommune inngikk med Evry 05. september 2014. Sømna kommune må betale for kommunikasjonsløsningen til ASP-avtalen, som er en ISP-linje (Internet Service Provider) med VPN (Virtual Private network) mellom kommunen sitt nettverk og Evry sine servere. Sømna kommune mottar faktura fra Evry på denne kommunikasjonsløsningen, på ca. 60 000 kroner i året.

I ASP-avtalen inngår drift og brukerstøtte for Agresso. Kommunen har en egen programvarevedlikeholdsavtale for Agresso med Unit4 Agresso. Kommunen mottar fakturaer fra Unit4 Agresso for ca. 66 000 kroner i året.

Brønnøy ivaretar det avtaletekniske i ASP-avtalen med Evry. Brønnøy fakturerer Sømna for tjenestene på vegne av Evry. I følge kostnadsfordelingen mellom kommunene basert på Evry-avtalen er Sømnas andel av prognoserte faste driftskostnader i 2017 ca. 417 000 kroner årlig. Kostnadsfordelingen mellom kommunene er basert på antall årsverk som SSB har registrert i kommunene i 2012. Sømnas andel er 15,8 prosent. Rådmann og IT-tekniker mener at disse programmene og supporten fra Evry fungerer greit.

På konto 124000 serviceavtaler/reparasjoner/vaktmestertjenester er det i perioden 1. januar til utgangen av september 2017 fakturert Sømna kommune følgende fra de omtalte leverandørene over:

- Evry ca 70 000 kroner
- Brønnøy kommune ca 104 000 kroner
- Unit4 Agresso 67 000 kroner

2.3 Avtale med IT Partner Helgeland

Sømna kommune undertegnet i desember 2015 avtale med IT Partner Helgeland AS om driftsteknisk støtte. Avtalen gjelder fra 01.12.15, med en varighet på seks måneder med automatisk fornyelse for seks måneder om gangen, hvis den ikke sies opp senest to måneder før utløpet av en avtaleperiode. Høsten 2016 ble det utarbeidet en ny avtale med IT Partner gjeldende fra 01.01.17. Avtalen er ved utgangen av november 2017 ikke signert.

Avtalene med IT Partner er i utgangspunktet lik, men unntak av oppdatering av utstyrsliste og endring av timebanken fra 10 til 20 timer pr måned. Kommunen opplyser at ønske om en såpass kort varighet skyldes muligheten for å kunne se avtalen litt an og eventuelt gjøre endringer underveis. I den nye avtalen var det behov for å legge inn flere timer support da den forrige avtalen ikke hadde tatt med tilstrekkelig antall timer i rammen i timebanken og dette ble forholdsvis kostbart.

Avtalen med IT Partner omfatter tjenestenivået *Respons med timebank*. Dette inneholder følgende tjenester:

- *Kompetansetilgang*: Kunden får tilgang på leverandørens kompetanse og kunnskap om driftstekniske problemstillinger. Leverandøren har kompetanse på nettverksløsninger, operativsystem og serverdrift på Microsoft og VMware plattform. Ved driftsveiledning knyttet til spesielle fagsystemer er leverandøren behjelpelig med eskalering i forhold til disse
- *Systemdokumentasjon*: Beskrivelse av virksomhetens tekniske organisering og oppbygging av IKT-systemene. Denne lagers på leverandørens sikre lagringsplattform, men eies helt og fullt av kunden. Leverandøren oppdaterer systemdokumentasjonen fortløpende gjennom hele avtaleperioden.
- *Responstid*: Ved kritiske feil er responstiden 4 timer og ved andre feil er den 8 timer, og responstiden gjelder innenfor normal arbeidstid 8.00-16.00. Med responstid menes tiden fra feilen er meldt per telefon eller epost, eller oppdaget via overvåkning av servere, og til feilretting er påbegynt.
- *Timebank*: Omfatter et visst antall timer som belastes per påbegynte halvtime ved oppdrag, support og lignende.

Den gamle avtalen med en timebank på 10 timer var priset til 14 550 kroner eks mva per måned, mens den nye avtalen er priset til 24 950 kroner eks mva per måned, inkludert en timebank på 20 timer. Bestilt arbeid utover avtale prises etter gjeldende prisliste.

Avtalen inneholder spesielle avtalevilkår som omfatter:

- Leverandøren er ansvarlig for drift, vedlikehold og videreutvikling av kundens server, nettverk infrastruktur og backup løsning. Feil eller behov for endringer skal meldes leverandøren.

- Kunden skal ha en (eller flere) definerte lokale IKT ressurser som skal ha ansvar for lokal brukerstøtte og enklere drifts- og vedlikeholdsoppgaver. Lokale brukere skal primært gå gjennom lokal IKT ressurs ved behov for bistand og lokal ITK ressurs vurderer hva som skal eskaleres til leverandør.
- Kunden får tilgang til leverandørens Service Desk som tar imot, registrerer og tar ansvar for å løse innmeldte saker.
- Det skal gjennomføres statusmøter fire ganger i året.

I oppstartsmøte ble det fortalt at kommunen har møter med IT Partner hver eller hver annen måned. Tema er status på saker i Sømna kommune, og kommunen informeres om hvilke saker IT Partner arbeider med. Revisor har fått tilgang til to møtereferat. Av referatet fra 23.08.2016 framgår det at *månedlig systemsjekk* er innført. Månedlig systemsjekk omfatter kontroll av maskinvare, operativsystem og sikkerhetssystem for å avdekke begynnende feilsituasjoner før det får konsekvenser for tilgjengeligheten av systemene. I tillegg kontrolleres sikkerhetssystemene slik som sikkerhetskopierings-logg, antivirusløsning, brannmur og andre sikkerhetsløsninger. Det framgår også av referatet at IT Partner skal gi tilbud på ProAktiv, både på selve innføringen og oppgradering av avtalen. ProAktiv er et nytt tjenestenivå i avtalen og omfatter en visualisering av virksomhetens IT-systemer på kontrolltavler plassert i leverandørens driftsmiljø, som overvåker de mest vitale parameterne i på tjenermaskiner og nettverksinfrastruktur i sanntid, slik at leverandøren kan reagere umiddelbart om avvik forekommer og handler etter fastsatte rutiner.

Referatet viser også at det er planer om at IT Partner skal ta ansvaret for å vedlikeholde forretningskritiske avtaler og at lisensiering er i henhold til lovverket. Dette omfatter Microsoft, VMware (backup), Veeam (antivirus), Trend AV, Fortigate (brannmur) og Adobe.

Det refereres også til en sak om behovet for å gjennomgå tilgangen til felles mapper for lege, psykiatri og helsestasjon fordi man har signaler på at dette ligger åpent i dag.

Av møtereferatene framgår det også at timebanken pr juli 2016 på 70 timer er overskredet med 167 timer.

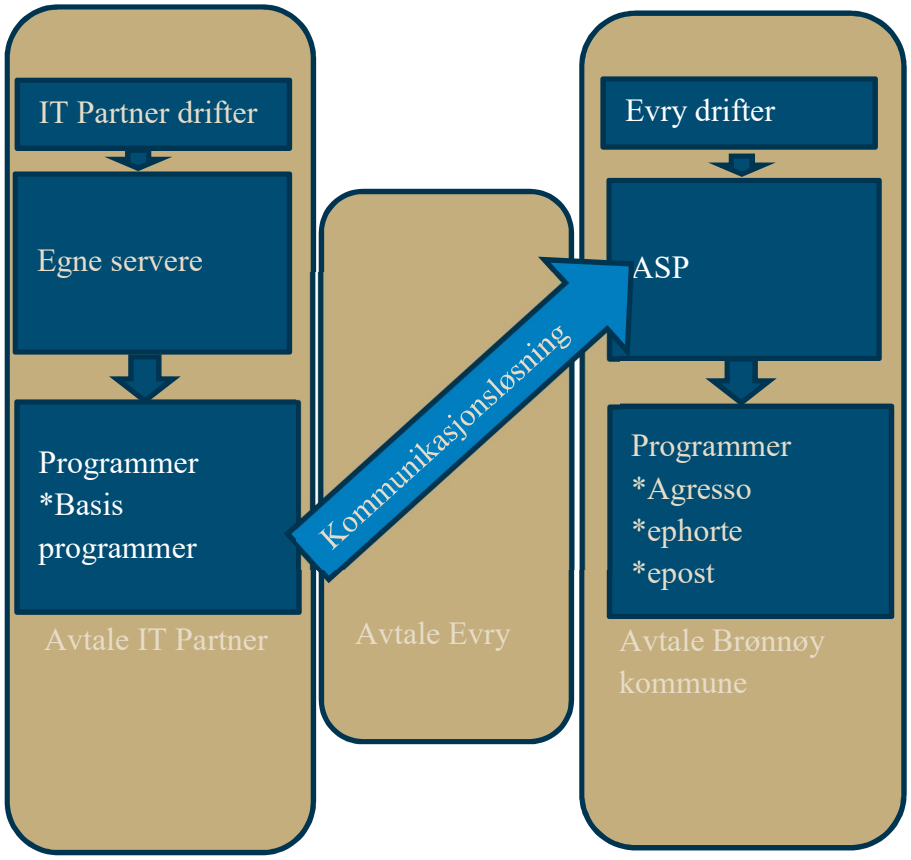
I møtereferatet fra 21.11.2016 fram går det at IT Partner skal se på mulighetene for å konsolidere IKT-systemet, fordi det opptar plass i datasenteret og medfører lisenskostnader. I tillegg er det en sak om norm for informasjonssikkerhet.

Kommunen får kvartalsvis fakturaer i henhold til avtalen og kan sjekke at det betales for gitte ytelser. IT Partner har til sammen fakturert Sømna kommune 349 622 kroner i perioden 01.01.2017 til 01.10.2017. I dette beløpet inngår en faktura på 201 615 kroner knyttet til oppgradering av lisenser. Selve avtalen har en årskostnad på ca. 300 000 kroner.

Avtalen med IT Partner fungerer ifølge rådmann og IT-tekniker greit. IT Partner tar seg av drift av nettverk og backup, og det er lett å ringe dem for å få hjelp. IT Partner har ekspertise på ulike områder, og firmaet oppfyller kommunens forventninger, og kommunen får hjelp når det trengs.

2.4 Oppsummering av avtaler

I figur 2.1 er det skissert en overordnet oversikt over IKT-relaterte avtaler og innholdet i dem. For økonomisystemet Agresso kommer i tillegg avtale om programvare-vedlikehold for Agresso med Unit4 Agresso. I tillegg til innholdet i avtalene under har kommunen også programvare hvor de betaler lisenser eller årlige avtaler med den enkelte programvareleverandør.



Figur 2.1: Oversikt over avtaler og innhold

3. PLANLEGGING OG ORGANISERING

3.1 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot. Når det gjelder planlegging og organisering har vi utledet følgende kriterier fra personopplysningsloven med tilhørende forskrifter, E-forvaltningsforskriften og COBIT:

Planlegging og organisering:

1. Kommunen skal ha en IKT-strategi som:
   - viser kommunens overordnede mål og hvordan IKT skal bidra til å nå målene
   - viser veivalg knyttet til IKT
   - viser konkrete handlingsplaner
2. Det skal etableres klare ansvars – og myndighetsforhold for bruk av informasjonssystemet. Disse skal være dokumentert, og endringer skal godkjennes av øverste myndighet.
3. Utstyr og program skal være sammenkoblet på en hensiktsmessig og sikker måte, og konfigurasjonen (informasjonssystemets utforming) skal dokumenteres.
4. Sensitive data skal ha høyere sikkerhetsnivå
5. Det skal gjennomføres og dokumenteres ROS-analyse for informasjonssikkerhet, og analysen skal klarlegge sannsynlighet for og konsekvenser av sikkerhetsbrudd.
6. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger. Resultatet av risikovurderingene skal sammenlignes med de fastlagte kriteriene for akseptabel risiko forbundet med behandling av personopplysninger
7. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten

3.2 Data

3.2.1 IT-strategi

En IKT-strategi skal vise kommunens overordnede mål og hvordan IKT skal bidra til å nå målene. Strategien skal videre vise veivalg knyttet til IKT og konkrete handlingsplaner på området.

Sømna kommune har ikke utarbeidet IKT-strategi. Rådmannen forteller at kommunen er forsinket med kommuneplanarbeidet. Sektorstrategier vil komme etterhvert, og

digitalisering er et av fem områder som rådmannen anser det er viktig å få på plass plan for. Rådmannen peker på at formannskapet muntlig har gitt uttrykk for at de forventer at det skjer noe på IKT-området i Sømna kommune. Dette vil bli fulgt opp av rådmannen og hans stab gjennom digitaliseringsarbeidet som startes opp våren 2017. Rådmannen har forventning om at strategien skal bringe Sømna videre på to områder: Digitalisering internt og mer effektiv forvaltning, og publikumstjenester på nett.

Formannskapet behandlet i møtet 13.09.2017 plan for digitalisering i Sømna kommune. Av rådmannens plan for digitalisering går det fram at innholdet i en digitaliseringsstrategi skal ta utgangspunkt i behovet for å identifisere områder hvor man skal satse på digitalisering framfor å gå veien om en egen digitaliseringsstrategi. Rådmannen peker videre på at dette er en framgangsmåte som er tilpasset kommunens størrelse, kapasitet, kompetanse og omstillingsbehov. Det pekes også i saksframlegget på at informasjonssikkerhet og behandling av persondata må ivaretas innenfor satsingen av digitalisering. Kommunens arbeid med sikkerhetsnorm omtales nærmere i kapittel 6.2.1.

Kommuneplanens samfunnsdel er lagt ut på 2. gangs høring 23.10.2017. Her omtales digitalisering som den mest omfattende teknologiske trenden i vår tid og den preger de fleste samfunnsområder. Utfordringen er å utnytte den digitale utviklingen for å være framtidsrettet. Kommunen som organisasjon skal være ledende innen digitalisering på Helgeland.

3.2.2 Myndighet og ansvar

Formell organisering

Sømna kommune har en person i 100 prosent stilling på IKT. Fra høsten 2017 har kommunen også en lærling på IKT. Stillingene er lagt til teknisk avdeling. I Sømna kommunes budsjett for 2017 og økonomiplan for 2017-2020 går det fram at teknisk har fått budsjettansvaret for IKT fra 2017. I kommunens organisasjonskart derimot, er IT plassert i sentraladministrasjonen i kommunen og ikke i teknisk avdeling. I høringssvaret fra kommunen, jfr. vedlegg 2 opplyses det at i den pågående organisasjonsgjennomgangen så skal kommunen ha på plass en digitaliseringsansvarlig i stab.

Dagens IT-tekniker har vært i stillingen i litt over ett år, og arbeider bare med IKT i kommunen. En annen ansatt på teknisk kan steppe inn ved sykdom, men dette er ikke en formell ordning. I tillegg har skolene 50 prosent stillingsressurs til å ta seg av IKT, men dette omfatter ikke den tekniske driften av IKT-systemet. IT-teknikeren har liten kontakt med dem.

Kommunen kjøper eksterne ressurser gjennom en avtale med IT Partner Helgeland og fra Evry, jfr. kapittel 2. Avtalen med ekstern IKT leverandør er godt kjent eller ganske godt kjent for 27 prosent av lederne i kommunen og 47 prosent av dem, er godt fornøyd

med samarbeidet med ekstern IKT-leverandør. Her er det usikkert hvilken av avtalene som respondentene har svart i forhold til. Kommentarene fra respondentene omhandler i stor grad support og en kommentar peker på at det er vanskelig å skille mellom hva som skal gå til lokal support og til ekstern support.

Roller og ansvarsfordeling IKT

I intervjuet med rådmann og IT-tekniker går det fram at det overordnede ansvaret for IKT-området ligger hos rådmannen, og dette er ikke delegert videre. IT-teknikeren er ansvarlig for koordinering og samordning av IKT-tjenestene. IT-tekniker har også sikkerhetsansvaret. Ansvarsfordelingen er ikke dokumentert. IT eller IKT omtales ikke i delegasjonsreglementet.

IT-tekniker har ansvar for lokal brukerstøtte, generelt klientoppsett og enklere drifts- og vedlikeholdsoppgaver. I tillegg er det er superbrukere for fagprogrammene ute på enhetene. Hver leder er superbruker på økonomisystemet Agresso. IT-tekniker er førstelinje for support og videresender eventuelt oppgaver som han ikke kan løse til IT Partner.

IT Partner er ifølge avtalen ansvarlig for drift, vedlikehold og videreutvikling av kommunens server, nettverk, infrastruktur og backupløsning. Switcher og servere er kommunens eiendom. IT Partner og eventuelle programleverandører er ansvarlig for kommunikasjon og programvare. I tillegg kommer support. Avtalen med IT Partner er i 2015 signert av eiendomssjefen, den nye avtalen som skulle tre i kraft fra 01.01.2017 er ikke signert. Avtalen fra 2015 er ikke behandlet i kommunestyret. Det framgår av referatene fra statusmøtene mellom Sømna kommune og IT Partner at IT Partner gjennom 2016 overtar eller har planer om å overta flere funksjoner knyttet til drift av kommunenes IKT-system.

Ansvars- og myndighetsforhold for bruk av informasjonssystemet er dokumentert gjennom brukernes tilganger i IKT-systemet gjennom AD (active directory). IT-teknikeren sier at de ansatte selv er ansvarlige for hvordan de bruker kommunens informasjonssystem. 62 prosent av brukerne oppgir at de er kjent med sitt ansvars- og myndighetsforhold for bruk av kommunens informasjonssystem, mens 21 prosent ikke vet. De som oppgir å kjenne sitt ansvars- og myndighetsforhold har blitt kjent med det gjennom tildeling av oppgaver (44 prosent) og gjennom samtale med overordnede (25 prosent).

Det er usikkert i hvilken grad de ansatte er kjent med rutiner og informasjonssikkerhet, men IT-teknikeren oppfatter at de ansatte er kritiske og forsiktige i sin bruk IKT-systemene. Informasjonssikkerhet er nærmere omtalt i kapittel 7.2.2 – 7.2.4.

I følge avtalen med IT Partner skal det gjennomføres statusmøter ca. fire ganger i året. Revisor har fått tilgang til tilfeldig utvalgte referater fra slike møter. Det framgår av møtereferatet at det behandles saker knyttet til ordinær drift og vedlikehold, sikkerhet

og endringer i driftsmiljøet. Det angis også frist for gjennomføring og hvem som er ansvarlig for gjennomføringen.

3.2.3 Informasjonsarkitektur

I henhold til personopplysningsforskriften § 2-7 skal informasjonssystemet konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås, og konfigurasjonen skal dokumenteres. Med konfigurasjon menes informasjonssystemets utforming, det vil si utstyr og program samt sammenkoblinger mellom disse. Ved valg av konfigurasjon skal virksomhetens behov for informasjonssikkerhet tillegges vekt, i tillegg til vurdering av økonomi og behov for funksjonalitet. Eksempelvis vil slik vurdering omfatte etablering av sikkerhetsbarrierer, bruk av nettverkssegmentering for å skille forskjellige behandlinger av personopplysninger fra hverandre i informasjonssystemet eller lignende.

Sømna kommune har en systemdokumentasjon som beskriver konfigurasjon, fjerndriftsløsning, oppbygging av nettverk, internt nett og switcher. Systemdokumentasjonen beskriver kommunens tekniske organisering av IKT-systemet, og lagres på IT Partner sin sikre lagringsplattform. IT Partner har ansvar for oppdateringer. Ved valg av løsning for organisering av nettverket ble det vektlagt å få en sikker sone lukket fra andre nett. Nettverkssikkerhet lå også til grunn for de øvrige valgene som kommunen har gjort på dette området, og IT Partner har foreslått og satt opp dette i samarbeid med kommunen. Serveren er beskyttet med passord i 3 trinn.

Sømna kommune har konfigurert nettverket med to brannmurer; en ytre og en indre. IT Partner er ansvarlig for oppgradering og vedlikehold av brannmurer. Sømna kommune benytter nettverkssegmentering, og sensitive data ligger i sikker sone bak en egen brannmur. IT Partner mener at IKT-systemet i kommunen nå er betraktelig bedre enn da de begynte å arbeide med det. Det tekniske og nettverk er bra i orden, men det mangler litt på rutiner.

IT Partner og kommunen er ansvarlig for virusbeskyttelse. Virusprogram og logg over antivirus driftes av IT Partner, mens lokal IT sørger for å stenge ned PCer ved behov. Ifølge IT-teknikeren fungerer samarbeidet godt samarbeid på dette området.

IT Partner gjennomfører systemsjekk med jevne mellomrom, noe som innebærer kontroll av maskinvare, operativsystem og sikkerhetssystem for å hindre feil som går utover tilgjengeligheten til systemene. Kontroll av sikkerhetssystemene omfatter kontroll av sikkerhetskopieringslogg, antivirusløsning, brannmur og andre sikkerhetsløsninger. Alle avvik dokumenteres og tiltak/forbedringer skal foreslås. Det lages en rapport til kommunen etter gjennomført systemsjekk. Månedlig systemsjekk er ikke tatt inn i avtalen og IT Partner opplyser at de gjennomfører systemsjekk med jevne mellomrom som en ekstra sikring.

Det framgår av referat fra kommunens statusmøte med IT Partner 21.11.2016, at IT Partner skal gi tilbud på innføring av ProAktiv og en oppgradering av avtale. ProAktiv innebærer visualisering av overvåkningen av de mest vitale parameterne i IT-systemet og vil være en automatisering av det som skjer i systemsjekk. Pr oktober 2017 er ikke ProAkiv iverksatt.

3.2.4 Risikostyring

En ROS-analyse skal fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger, og klarlegge sannsynlighet og konsekvenser av sikkerhetsbrudd.

Det er gjennomført risiko- og sårbarhetsanalyse (ROS-analyse) i 2013, men denne anses å være utdatert. 40 prosent av lederne oppgir at kommunen har gjennomført en ROS-analyse som gjelder informasjonssikkerhet, mens 47 prosent ikke vet. De lederne som har svart (n=5) oppgir at det er mer enn 2 år siden eller at det ikke vet når siste ROS-analyse ble gjennomført.

Kommunen har plan for krisehåndtering (kommunal kriseledelse), men denne omhandler ikke IKT. Hvis en fiberkabel ryker, har kommunen egen linje til legekontoret som ligger i samme bygg som sykehjemmet. På grunn av at serveren ligger lokalt, har de som trenger det tilgang til journalsystem uansett. Det finnes også et nødstrømsaggregat på sykehjemmet. Hvis det oppstår brudd mellom kommunehuset og sykehjemmet, rettes dette ifølge IT-teknikeren ganske fort.

I kartleggingen av IT-miljø (datert 02.01.2017) vurderes strømbrudd som en vesentlig risiko på IT-området. For å redusere risikoen planlegger kommunen å flytte datasenteret til sykehjemmet hvor det finnes et nødstrømsaggregat.

Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. I intervjuet pekte IT-teknikeren på at feilhåndtering av datasikkerhet er et eksempel på hendelse som kan utløse ny ROS-analyse. I spørreundersøkelsen mener lederne at innkjøp av ny programvare, endringer i risikobildet, for eksempel virusangrep og nye samarbeidsparter innenfor IKT er de forhold som i størst grad krever risikovurdering/ ny ROS-analyse.

Av lederne i kommunen er det 20 prosent som oppgir at kommunen har definert akseptabel risiko forbundet med behandling av personopplysninger, mens 53 prosent ikke vet.

3.3 Vurdering

IT-strategi

Det foreligger ingen IT/IKT-strategi i Sømna kommune som viser overordnede mål, veivalg knyttet til IKT og handlingsplaner. Det arbeides med en digitaliseringsstrategi

som en sektorstrategi til samfunnsplan. Denne digitaliseringsstrategien ser i hovedsak ut til å være rettet mot digitalisering av tjenester rettet mot publikum og digitalisering av arbeidsoppgaver internt i kommunen og revisor mener at den ikke ser ut til å dekke viktige områder som forventes i en IKT-strategi. En IKT-strategi vil danne grunnlag for valg av løsninger, rutiner og sikkerhetspolicy innenfor IKT samt klargjøre og dokumentere ansvar- og myndighetsforhold. Slik arbeidet med digitaliserings-strategien er lagt opp velges det ut noen områder hvor arbeidet startes opp uten forutgående strategiske valg av hva som skal gjøres. Revisor oppfatter at denne tilnærmingen kan føre til at viktige områder ikke blir ivaretatt i strategien.

Myndighet og ansvar

Kommunens IT-tekniker er i praksis organisert under kommunalsjef teknisk, eiendom. I organisasjonskartet for kommunen er derimot IT en enhet i sentraladministrasjonen. Dette framstår som uryddig. Rådmann har det overordnede ansvaret for bruk av informasjonssystemet og dette er ikke delegert. I tillegg til interne ressurser kjøpes det ressurser gjennom en avtale med IT Partner til drift av IKT-systemet. IT-teknikeren har overordnet operativt ansvar for koordinering og samordning, mens overordnet ansvar for drift ligger til IT Partner.

Avtalen med IT Partner er lite kjent i organisasjonen og dette kan blant annet føre til at ansatte har liten innsikt i for eksempel hvordan arbeidsfordelingen mellom lokal brukerstøtte (IT-tekniker) og brukerstøtte fra IT Partner er ment å fungere. Selv om arbeidsdelingen mellom IT Partner og IT-teknikeren er tydelig for de involverte ser den ikke ut til å være dokumentert slik at andre kan forholde seg til den. Det er også et delt ansvar mellom IT-teknikeren og IT Partner når det gjelder sikkerhet og dette er avgrenset til at IT-teknikeren foretar de nødvendige nedstenginger av maskiner etter beskjed fra IT Partner. Denne arbeidsdelingen er tydelig. Samtidig er det slik at IT-tekniker har sikkerhetsansvaret som går ut over det rent tekniske. Det vil si tilganger til IKT-systemer og definering og behandling av sensitive data.

Endringer i ansvars- og myndighetsforhold skal godkjennes av øverste myndighet. Det er ingen skriftlige rutiner eller dokumentasjon av ansvars- og myndighetsforhold for bruk av informasjonssystemet. Brukernes rettigheter framgår av de tilgangene som hver enkelt har, men dette er ikke dokumentert ut over at tilgangene finnes i AD (Active Directory). Revisor er ikke kjent med at det finnes retningslinjer for hvem som skal ha hvilke rettigheter.

Informasjonsarkitektur

Informasjonssystemet skal være sammenkoblet med utstyr og program på en hensiktsmessig måte. Så langt revisor kan vurdere ser det ut til at det eksisterende informasjonssystemet er sammenkoblet på en hensiktsmessig og sikker måte med brannmurer, virusprogram og nettverkssegmentering, og informasjonssystemet er dokumentert. Gjennom nettverkssegmentering er sensitive data adskilt fra andre deler av informasjonssystemet.

Risikostyring

Kommunen har ikke oppdatert ROS-analysen fra 2013. Kommunen har fått nye samarbeidsparter innenfor IKT, mest sannsynlig kjøpt inn ny programvare siden 2013 og mest sannsynlig opplevd eksterne trusler siden 2013, som er de forholdene som flest ledere mener krever ny ROS-analyse. Mye tyder på at kommunen ikke har definert en akseptabel risiko forbundet med behandling av personopplysninger. I ROS-analysen fra 2013 finner vi at tiltaksgrensen der settes til 11 (sannsynlighet x konsekvens), før det bør iverksettes tiltak for å redusere sannsynlighet eller konsekvens. Det er ikke spesifisert et eget akseptabelt nivå for behandling av personopplysninger. Revisor mener at metodikken fra ROS-analysen i 2013 kan videreføres, men ROS-analysen fra 2013 må oppdateres.

4. ANSKAFFELSER OG IMPLEMENTERING

4.1 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot. Når det gjelder anskaffelse og implementering har vi utledet følgende kriterier fra personopplysningsloven med tilhørende forskrifter, E-forvaltningsforskriften og COBIT.

Anskaffelse og implementering:

1. Kommunen bør ha utarbeidet en kravspesifikasjon til sin leverandør før anskaffelser innen IKT.
2. Kommunen bør ha en plan for investering og utskifting av maskinvare (pc, servere, utstyr til nettverk etc).
3. Kommunen bør ha en plan for investering i og vedlikehold av programvare, og sørge for at kommunens programvare til enhver tid er oppdatert.
4. Kommunen bør sørge for at installasjon og implementering av systemer utføres av kompetent personell.

4.2 Data

4.2.1 Kravspesifikasjon

I avtalen med IT Partner framgår det hva som skal vedlikeholdes/driftes og hvilket utstyr som omfattes av avtalen (utstyrsbeskrivelse). Revisor har ikke fått tilgang til kravspesifikasjon som lå til grunn for avtalen med IT Partner og antakelig lå det ingen kravspesifikasjon til grunn for avtalen. Verken rådmann eller IT-tekniker har kunnskap om historien bak avtalen med IT Partner og eventuelle valg som ligger til grunn for den. Fra IT Partner oppgis det at samarbeidet mellom kommunen og IT Partner startet i forkant av den første avtalen som ble signert i desember 2015 fordi kommunen trengte hjelp.

I IT-teknikerens kartleggingen av IT-miljø (datert 2. januar 2017) går det fram at kommunen oppgraderer kontinuerlig systemer slik at de til enhver tid fungerer optimalt.

4.2.2 Anskaffelse og vedlikehold av teknologisk infrastruktur

Sømna kommune har ansvar for anskaffelse av maskiner selv. I intervju peker rådmannen og IT-teknikeren på at IT Partner har vært med på anskaffelse av servere til kommunen. Ved anskaffelser er driftssikkerhet ett av de viktigste kriteriene i kravspesifikasjonen, vurderingen gjøres av IT-teknikeren. Kommunen har oversikt over servere og switchere, men ikke over PC parken. PC parken anses å være bra og

oppdatert, og IT-teknikeren mener det er behov for mindre oppgraderinger framover. IT Partner mener at kommunen snart nærmer seg behov for utskifting av den plattformen som IKT-systemet er bygd på. Det framgår av referater fra statusmøter mellom IT Partner og kommunen at det arbeides med en konsolidering av IKT systemet, men det foreligger ingen konkret plan.

IT Partner har også foreslått og satt opp nettverkskonfigurasjonen i samarbeid med kommunen. IT-tekniker har mulighet til å sette inn nye enheter i nettverket.

4.2.3 Anskaffelse og vedlikehold av programmer og applikasjoner

Ved anskaffelse av større fagspesifikke programmer ligger beslutningen hos rådmannen. Hvis en enhet ønsker ny programvare betyr det faglige skjønnet mye og behovet settes opp mot økonomisk ramme. For eksempel var det i mars 2017 et ønske fra kommunalsjefen og skolene å anskaffe et skoleadministrativt system. De har pekt på programvaren de ønsker, men kommunen har ikke kommet så langt at anskaffelsen er vurdert opp mot økonomi og lov om offentlige anskaffelser.

Når det gjelder programvare er mye moderne, og IT-teknikeren ser ikke behov for snarlig oppgraderinger.

Det er som regel IT Partner som sørger for at program som ligger på server er oppdatert og som sørger for oppdateringer av servere. Vedlikehold og oppdateringer av basis programvare som alle brukere må ha, er ifølge referat fra statusmøter mellom IT Partner og kommunen delvis overlatt til IT Partner. For noen programmer er det programleverandøren som gjør dette, spesielt ved tyngre program. Unntaket er at IT-teknikeren sørger for oppdatering av programmet Gerica med bistand fra IT Partner. IT-teknikeren gir beskjed til de ansvarlige når det er behov for øvrige oppdateringer.

Når det leveres spesialprogram må den som skal ha programmet ta ansvar i forbindelse med oppstart, herunder sørge for å få opplæring.

Ansatte kan selv legge inn programmer på egen PC. Mange systemer krever at bruker kan gjøre mye selv og IT-tekniker mener at for store restriksjoner her gjør at det blir for mange begrensninger for eksempel ved oppdateringer. Det er gjort vurdering på den enkeltes frihetsgrader, og kommunen ønsker å begrense den enkeltes muligheter bare der det er behov for slik kontroll.

4.2.4 Installasjon og godkjenning av systemer

Det er IT Partner eller programleverandøren som installerer nytt utstyr og programvare. IT-teknikeren følger opp leveransen lokalt ved blant annet å teste maskin med programvare før den leveres ut til sluttbruker.

I kartleggingen av IT-miljø oppgis det at alle berørte gis beskjed i forkant av endringer av IT-løsninger, oppdateringer og lignende. Videre tas det backup før endringen utføres.

4.3 Vurdering

Kravspesifikasjon

Kommunen bør ha utarbeidet en kravspesifikasjon til sin leverandør før anskaffelser innen IKT. Revisor har ikke klart å finne fram til vurderinger som ligger bak valg av løsning for kommunens IKT-system og heller ikke grunnlaget for valg av leverandør.

Plan for anskaffelse og vedlikehold av maskinvare

Kommunen bør ha en plan for investering og utskifting av maskinvare (PC, servere, utstyr til nettverk). Kommunen har ikke oversikt over PCer og ingen plan om utskifting av PCer bortsett fra mindre oppgraderinger. PCer varer ikke evig og uten en plan kan kommunen risikere at det plutselig oppstår et stort behov for utskifting av PCer. IT Partner melder også om at behovet for å skifte ut plattformen som IKT-systemet er bygd på vil melde seg om noen år. En plan vil også gjøre det mulig å budsjettere investeringer i forhold til behovet. Gjennom systemdokumentasjonen (i avtalen med IT Partner) har kommunen oversikt over servere og andre nettverksressurser i IT-systemet og dette danner grunnlag for vurderinger av behovet for vedlikehold og oppgraderinger.

Plan for anskaffelse og vedlikehold av programvare

Kommunen bør ha en plan for investering i og vedlikehold av programvare, og sørge for at kommunens programvare til enhver tid er oppdatert. Det finnes ingen plan for investering i og vedlikehold av programvare. Vedlikehold og oppgraderinger av programvare styres i stor grad av programvareleverandører. Investeringer gjøres etter en behovsvurdering i forhold til budsjettet.

Installasjon og godkjenning av systemer

Kommunen bør sørge for at installasjon og implementering av systemer utføres av kompetent personell. Så langt revisor kan vurdere framstår IT Partner som en kompetent bedrift som kan sørge for installasjon og implementering av systemer. Noen programvareleverandører vil også bistå med installasjon og implementering av systemer.

5. DRIFTSLEVERANSE OG STØTTE

5.1 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot. Når det gjelder driftsleveranse og støtte har vi utledet følgende kriterier fra personopplysningsloven med tilhørende forskrifter, E-forvaltningsforskriften og COBIT.

Driftsleveranse og støtte:

1. Forventet servicenivå skal være definert i avtale med leverandør, herunder oppetid på systemet og responstid for bistand, rapportering fra leverandør.
2. Brukere skal gis opplæring i bruk av systemet (alle funksjonaliteter i systemet).
3. Ansatte skal ha kjennskap til retningslinjer og rutiner for informasjons-sikkerhet.
4. Det skal være etablert et system for registrering av feilmeldinger og hendelser.
5. Systemet skal bidra til at innmeldte feilmeldinger og hendelser blir fulgt opp.
6. Autorisert bruk av systemet skal dokumenters gjennom en aktivitetslogg.
7. Serverrom skal være sikret fysisk mot uautorisert adgang.

5.2 Data

5.2.1 Servicenivå

Kommunen anser rask og riktig hjelp, og at problemer løses, som vesentlig for servicenivået fra IT Partner. Responstiden er beskrevet i avtalen, men ikke oppetid. Med responstid menes tiden fra feil er meldt pr telefon eller epost, eller oppdaget via overvåking av servere, og til feilretting er på begynt. Responstiden gjelder innenfor normal arbeidstid 08:00-16:00. Ved kritiske feil er responstiden 4 timer og ved andre feil er responstiden 8 timer. I avtalen ligger det ingen bestemmelser på tilgjengelighet ut over ordinær arbeidstid, men IT Partner oppgir at kommunen vil få tak i folk i en krisesituasjon. I slike tilfeller tar IT Partner et utrykningshonorar.

Kommunen måler ikke servicenivået. IT-teknikeren sjekker gjennom logger hvordan avtalen overholdes med tanke systemsjekk for maskinvare, operativsystem og sikkerhetssystem.

Kommunen har gjennom ASP-avtalen med Brønnøy kommune brukerstøtte på Agresso, ephorte og epostsystemet. Av avtalen mellom Evry og Brønnøy kommune,

framgår det at driftstjenestene skal være regulert av en SLA (Service Level Agreement) med garantert oppetid innenfor normal arbeidstid med mulighet til utvidelse til 24/7/365. For brukerstøtte har kommunen tilgang til brukerstøttesystemet via til enhver tid gjeldende kanaler for registrering av supportsaker samt benytte systemet som en kunnskaps- og erfaringsbase til egen kompetanseoppbygging. Brukerstøtte ytes alle virkedager 8-16. Responstiden for kritiske feil er 2 arbeidstimer, for alvorlige feil 6 arbeidstimer og for mindre alvorlige feil 12 arbeidstimer. Brukerstøtte defineres her som bistand med brukerproblemer enten de skyldes feil eller manglende kunnskap hos brukerne.

Spørreundersøkelsen viser at 96 prosent av ansatte er helt enig, enig eller delvis enig i at kommunens IKT-system er tilgjengelig i arbeidstiden, mens de resterende har svart verken eller.

Det genereres ulike logger i IKT-systemet og IT-tekniker sjekker ikke logger uten at det er varsel om avvik. I tillegg følger også IT Partner med i bakgrunnen.

Det er sendt ut e-post til brukere om at de gir beskjed om IT-systemene ikke fungerer. Responsen er liten og IT-tekniker oppfatter at det er en normalsituasjon på supporthenvendelser. IT Partner uttrykker også at omfanget av supporthenvendelser fra Sømna kommune er som forventet og at IT-tekniker tar mer av support-henvendelsene nå enn tidligere.

IT-tekniker kan rykke ut ved kriser og IT Partner er alltid tilgjengelig på telefon.

5.2.2 Brukeropplæring

Brukerne skal gis opplæring i bruk av systemet og ansatte skal ha kjennskap til retningslinjer og rutiner for informasjonssikkerhet I intervjuet opplyses det at ved innføring av nye systemer gjennomføres felles opplæring, og dette anses som viktig for å utnytte investeringen. Det er ikke rutiner for hvordan nyansatte skal få innføring i kommunens systemer. Ved nyansettelser vises den nyansatte hvordan passord skal endres, og det er ikke noe opplæring utover dette.

Fra spørreundersøkelsen framgår det at 78 prosent av de ansatte har fått opplæring i IKT-systemet og 87 prosent av disse er helt enig, enig eller delvis enig i at opplæringen i IKT-systemet har vært tilstrekkelig. Når det gjelder opplæring i programmer oppgir 82 prosent at de er helt enig, enig eller delvis enig i at de har fått opplæring. Av de som har fått opplæring i programmer mener 91 prosent (helt enig, enig og delvis enig) at opplæringen var tilstrekkelig. Når det gjelder informasjonssikkerhet er 48 prosent av de ansatte enig eller delvis enig i at de har fått opplæring. Av disse er 66 prosent enig eller delvis enig i at opplæringen har vært tilstrekkelig.

Fra kartleggingen av IT-miljø i kommunen, oppgis det at kommunen sender ut månedlige informasjonseposter for å holde ansatte oppdatert på IKT-systemene og informasjonssikkerhet.

5.2.3 Uønskede hendelser og problemer

Det skal være etablert et system for registrering av feilmeldinger og hendelser, og systemet skal bidra til at innmeldte feilmeldinger og hendelser blir fulgt opp. Det meste av feilmeldinger blir registrert i lokal help-desk, som kommer inn via epostadressen support@somna.kommune.no. Det lokale help-desk-systemet er ment som førstelinje for support. Sakene registreres automatisk og løses etter hvert, men det som anses som kritisk prioriteres først. Den lokale help-desken fungerer i stor grad som en aktivitetslogg, slik at man har oversikt over arbeidsoppgaver. Svar fra lokal help-desk sendes fra IT-tekniker (ikke help-desken) til den som har gjort henvendelsen. Revisor har sett dokumentasjon på slik henvendelse, og innmelder får en kort tilbakemelding på hendelsen.

Sømna kommune har tilgang til IT Partner sin Service Desk (også kalt brukerstøtte), som tar imot, registrerer og tar ansvar for å løse innmeldte saker. I avtalen med IT Partner heter det at lokale brukere skal primært gå gjennom lokal IKT-ressurs ved behov for bistand, og lokal IKT-ressurs vurderer hva som skal eskaleres til leverandør.

De ansatte i Sømna kommune har fått en e-post om hvordan de skal forholde seg til IT Partner for å få hjelp. IT-teknikeren ringer som regel til IT Partner for brukerstøtte slik at han får raskt svar. Denne løsningen omfatter imidlertid ikke øvrige brukere. I praksis er det slik at noen brukere henvender seg direkte til IT Partners brukerstøtte. IT-tekniker ønsker ikke at andre ringer til IT Partner direkte, fordi ha ønsker at feilmeldinger skal kanaliseres via han for å vite hva IT Partner gjør.

Revisor har også sett dokumentasjon på henvendelse videreformidlet av IT-tekniker til ekstern brukerstøtte. Det framgår av dokumentasjonen at disse henvendelsene registreres med saksnummer og løsning på hendelsen beskrives kort i svaret til innmelder. IT-tekniker får løpende rapport over supportsaker som IT Partner behandler. IT Partner er god på driftsstøtte, IT-teknikeren forteller at kommunen er veldig godt fornøyd med hjelpen. Han får alltid tak i noen som kan hjelpe, selv om det ikke er den faste kontaktpersonen.

I ASP-avtalen med Evry ligger det inne brukerstøtte for de programmene som inngår i avtalen.

I spørreundersøkelsen til ansatte er 76 prosent[4] kjent med hvordan de kommer i kontakt med brukerstøtte. Her kan det variere hvilken brukerstøtte (IT-tekniker, IT Partner

[4] Hvis annet ikke er oppgitt er svarene basert på de som har svart at de er helt enig, enig eller delvis enig.

eller Evry) som brukerne har svart i forhold til. 59 prosent er enig i at det er lett å komme i kontakt med brukerstøtte og 52 prosent mener det er enkelt å forklare problemet til brukerstøtte. 65 prosent kontakter brukerstøtte når de opplever problemer i forbindelse med kommunens IKT-system. De som ikke kontakter brukerstøtte benytter seg av lokal IKT-ressurs (53 prosent), kollega (41 prosent) eller forsøker å løse problemene selv (6 prosent).

Det er 69 prosent som opplever at de får hjelp når de kontakter brukerstøtte. 60 prosent opplever at de får rask hjelp fra brukerstøtte ved kritiske feil og 59 prosent opplever at de får rask hjelp ved andre feil.

I kvalitetssystemet Compilo er det mulig for brukerne å melde avvik. Dette systemet genererer ikke beskjed om innmelding av avvik og IT-teknikeren opplever det for tungvint å gå inn på systemet for å sjekke, så det blir ikke gjort. Det som skjer i praksis er at IT-tekniker får en telefon hvis sakene blir liggende der for lenge.

5.2.4 Håndtering av data

Autorisert bruk av systemet skal dokumenters gjennom en aktivitetslogg. Det er sentralt at ansatte kun bruker informasjonssystemet for å utføre pålagte oppgaver og er autorisert for slik bruk. Det er også et krav at autorisert bruk av informasjons-systemet skal registreres.

Ansattes tilganger i IKT-systemet er styrt av AD (Active Directory) og leder bestemmer hva den enkelte skal ha tilgang til. I AD finnes oversikt over hvem som har tilganger til hva. I spørreundersøkelsen oppgir 89 prosent at de er helt enig, enig eller delvis enig i at de bare har tilgang til programmer som er nødvendig for den stillingen de har.

I intervju sier IT-tekniker at en logg på serveren viser dataaktiviteten, men at ingen sjekker denne. Noe aktivitet vil også kunne vises på brannmurene. IT-tekniker oppgir at det ikke har blitt registeret uønsket atferd på kommunens datasystemer.

Konfidensialitet, integritet og tilgjengelighet på data er nærmere behandlet i kapittel seks.

5.2.5 Fysiske omgivelser

Serverrom skal være sikret fysisk mot uautorisert adgang. Sømna kommunes servere er plassert i låst rom i kjelleren på kommunehuset. Nøkler oppbevares av IT-teknikeren og eiendomssjefen. Varmepumpe blåser kaldluft inn i rommet, og det er montert kamera med temperaturmåler i rommet. Kommunen har ingen andre servere, men har NAS (nettverkslagring) på sykehjemmet. IT-Partner mener at data som lagres på sykehjemmet er greit sikret. Rommet på kommunehuset har vindu og er således ikke innbruddssikkert. På sykehjemmet er det nødstrømsaggregat, men ikke primært for IKT-systemet. Kommunehuset mangler nødstrøm.

Sømna kommune har gjennom avtalen med Evry også data som lagres utenfor kommunen gjennom en ASP-løsning, hvor program ligger på nettet, men oppleves å ligge lokalt. Kommunen er ikke kjent med hvor Evry har sine servere. Datamateriale fra øvrige Helgelandskommuner viser at Evry har sine servere fysisk plassert i tre datahaller hvorav to er plassert i fjell. I datahallen kontrolleres temperatur og luftfuktighet, og overvåkes med tanke på vannskade og brann. Datahallen har høy fysisk beskyttelse mot adgang for uvedkommende.

5.3 Vurdering

Servicenivå

Forventet servicenivå skal være definert i avtale med leverandør, herunder oppetid på systemet og responstid for bistand, rapportering fra leverandør. I avtalen med IT Partner er responstid fra brukerstøtte hos IT Partner oppgitt, men ikke oppetid på systemet. I ASP-avtalen med Evry er oppetid og responstid definert. Brukerne ser ut til å være tilfreds med oppetid på IKT-systemet og responstiden hos brukerstøtte. Nå er det litt uklart om brukerne svarer i forhold til lokal help-desk (IKT tekniker) eller ekstern brukerstøtte hos IT Partner eller Evry, men samlet er det et tilfredsstillende servicenivå. IT Partner dokumenterer henvendelsene med saksnummer slik at det er mulig å følge opp og hente ut rapporter. Avtalen med IT Partner er lite kjent blant lederne slik at lederne kanskje ikke vet hva de kan forvente av service. Til tross for dette er de fleste lederne fornøyd eller har ingen mening om samarbeidet.

Brukeropplæring

Brukerne skal gis opplæring i bruk av systemet og bruken av systemet skal skje i samsvar med fastlagte rutiner. Ansatte får opplæring, men ikke alle har oppgitt at de får opplæring. En større andel av de ansatte har fått opplæring i IKT-systemet og programvare enn i informasjonssikkerhet. Revisor har ingen kunnskap om det er forskjeller mellom ulike enheter i kommunen. Det er ikke undersøkt nærmere om hvem som har ansvar for å gi opplæringen. Vi har opplysninger om at når det gjelder spesialprogrammer, så har brukeren selv et ansvar for opplæringen. Det sendes også ut epost med informasjon til ansatte for å holde dem oppdatert. Det er usikkert i hvilken grad slik epost når fram til de som er brukere av IKT-systemet, men som ikke har egen epostadresse.

Den enkeltes bruk av systemet styres av leder og de aller fleste oppgir at de bare har tilgang til de systemene som de trenger. Revisor kan ikke se at det finnes dokumenterte rutiner for bruken av systemet.

Ansatte skal ha kjennskap til retningslinjer og rutiner for informasjonssikkerhet. Kommunen arbeider med en sikkerhetsnorm (jfr. Kapittel 6.2.1), slik at det ennå ikke finnes rutiner for informasjonssikkerhet. Knapt halvparten av brukerne har fått

opplæring i informasjonssikkerhet. Revisor oppfatter at ansattes kjennskap til retningslinjer og rutiner for informasjonssikkerhet er mangelfull.

Uønskede hendelser og problemer

Det skal være etablert et system for registrering av feilmeldinger og hendelser og systemet skal bidra til at innmeldte feilmeldinger og hendelser blir fulgt opp. Support til brukerne av systemet er bygd opp i to trinn. Først en henvendelse til IT-teknikers help-desk og så videre til brukerstøtte hos IT Partner hvis IT-tekniker ikke kan løse problemet. Innboksen i lokal help-desk fungerer som en logg på henvendelser, men sakene videresendes/besvares ikke fra denne epostadressen. Hos IT Partner får henvendelsene egne saksnummer for oppfølging. Brukerne er stort sett fornøyd med den oppfølgingen de får på sine henvendelser. I tillegg har Evry brukerstøtte for programmer som ligger i ASP-løsningen. Det er noe uklart for brukerne hvordan arbeidsfordelingen mellom IT-tekniker og IT Partner er når det gjelder brukerstøtte, fordi noen brukere henvender seg direkte til IT Partner. Dette kan igjen forklare at kommunens timebank for brukerstøtte fra IT Partner overskrids. Revisor mener at kommunen har et tilfredsstillende system for registrering og oppfølging av feilmeldinger. Utfordringen er å informere brukerne om arbeidsfordelingen mellom IT-teknikeren og IT Partner.

Håndtering av data

Autorisert bruk av systemet skal dokumenters gjennom en aktivitetslogg. Det genereres aktivitetslogger i IKT-systemet, men revisor kan ikke se at det finnes rutiner for oppfølging av loggene ut over avvik som genereres. Gjennom kvalitetssystemet er det etablert et system for mottak og behandling av uønskede hendelser knyttet til bruk av IKT-systemer.

Fysiske omgivelser

Serverrom skal være sikret fysisk mot uautorisert adgang. Kommunens server er lokalisert i kjelleren på kommunehuset med varmepumpe for kaldluft og kamera med temperaturkontroll. Nøkler oppbevares av IT-tekniker og hans overordnet. I kjelleren på sykehjemmet er det nettverkslagring. Gjennom avtalen med Evry lagres data i gode omgivelser. Revisor mener at kommunens serverrom er tilstrekkelig sikret fysisk mot uautorisert adgang.

6. KONTROLLTILTAK

6.1 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot. Når det gjelder kontrolltiltak har vi utledet følgende kriterier fra personopplysningsloven med tilhørende forskrifter, E-forvaltningsforskriften og COBIT.

Kontrolltiltak:

1. Kommunens internkontroll(tiltak) på området skal vedlikeholdes
2. Kommunens internkontroll (tiltak) skal være kjent for medarbeiderne
3. Dataenes konfidensialitet skal være sikret:
   - Det skal være etablert tiltak som hindrer uautorisert personell tilgang til sensitiv/gradert informasjon
   - Det skal etableres et system for tilgangskontroll
   - Tilgangskontroll skal være tilpasset slik at bruker ikke gis tilgang til andre opplysninger enn vedkommende har bruk for i sin stilling
   - Tildeling av passord bør styres av en formell administrasjonsprosess
   - Det skal være rutiner for endring av passord
   - Det skal være etablert rutine for fjerning av tilganger for midlertidige brukertilganger og brukere som slutter
4. Dataenes integritet skal være sikret:
   - Det skal være mulig å oppdage forsøk på uautorisert bruk av informasjonssystemet
   - Rettigheter til å endre data skal være koblet til delegert myndighet
   - Tiltakene skal ikke kunne påvirkes eller omgås av medarbeiderne
5. Dataenes tilgjengelighet skal være sikret gjennom etablert backup rutiner og det skal være en reserveløsning for å ivareta kritiske data.

6.2 Data

6.2.1 Internkontroll

Kommunens internkontroll på IKT skal vedlikeholdes og den skal være kjent for medarbeiderne. Internkontroll er rådmannens ansvar. Gjennom IT Partner har Sømna kommune overvåking av maskinvare, operativsystem og sikkerhetssystem. En slik overvåking er en del av internkontrollen.

Avsnitt 3.2.4 omtaler en ROS-analyse fra 2013. Denne ligger ifølge våre informanter i kvalitetssystemet Compilo. Informantene peker på at det vil være mulig å legge IKT-kjøreregler og -rutiner i Compilo med signeringskrav. Dette er ikke gjort pr dato.

IT-teknikeren peker på at han gjennomfører egne kontroller med tanke på sikkerhet, men ingen ting er nedskrevet. Eksempel på slik handling er at IT-tekniker kontrollerer innstillinger på PC når han er ute hos bruker og gjennomgår sikkerhetslogg for antivirus. Det sendes ut eposter til brukere med orientering om potensielle sikkerhetstrusler.

Kommunen har ingen sikkerhetsstrategi, men arbeidet med sikkerhetsnorm var i startfasen våren 2017. I dette arbeidet skal områdeledere på helse og omsorg, legekontor, skole og NAV være med. Rådmannen kan ikke si noe om når arbeidet vil bli ferdig og pr mars 2017 er det bare gjennomført formøter. Det har ikke vært noen framdrift i arbeidet fram til oktober 2017. Normen vil bli lagt fram for politisk behandling når den er ferdig. Det gjennomføres ikke sikkerhetsrevisjon, men det er en oppfatning av at generell sikkerhet vurderes når flere elementer tas inn i driftsmiljøet.

6.2.2 Sikring av konfidensialitet

Sikring av konfidensialitet betyr at det skal være etablert tiltak som hindrer uautorisert personell tilgang til sensitiv/gradert informasjon og at det finnes et system for tilgangskontroll som gir den enkelte bruker tilgang til bare det vedkommende har bruk for i sin stilling samt at tilganger fjernes når brukere slutter. Sikring av konfidensialitet omfatter også tildeling av passord og rutiner for endring av passord.

Grupperegler i AD (Active Directory) styrer hvilke mapper og/eller systemer brukeren skal ha tilgang til. Tilgangen er også definert av hvor den enkelte bruker fysisk er plassert. Eksempelvis er det slik at helse- og omsorgssjefen ikke kan sitte på kommunehuset og logge inn på program som tilhører sykehjemmet. Sømna kommune har nettverkssegmentering og sensitive data ligger på sikker sone. I følge referat fra statusmøte mellom IT Partner og kommunen 23.08.2016, påpekes det behov for en gjennomgang av tilgangen til mapper innenfor lege, psykiatri og helsestasjon. Det er lite fokus på sikring av personopplysninger og sensitive data.

IT-teknikeren har oversikt over alle tilganger, han kan gå inn i AD (Active Directory) for å se tilgangene. Det finnes ikke noen egen skriftlig oversikt over tilgangene ut over det som finnes i AD. Rådmannen har tilgang på alt i administrasjonsnettet. Det er leder som bestemmer hvilke data den enkelte skal ha tilgang til og tilgang bestilles av den enkeltes leder. Det er også slik at bare brukere som disponerer PC-en får tilgang fra denne PC-en. Dersom ansatte skal ha tilgang til annen PC enn sin egen, må de ta kontakt med IT-teknikeren. Det er aldri gitt tillatelse til andre for å logge inn på en PC uten samtykke fra områdeleder eller etter direkte avtale med eier at brukerkontoen på den aktuelle PC-en. I intervjuet oppgis det at når noen slutter, deaktiveres alle tilganger med en gang, mens e-post blir stående ca. en uke før kontoen stenges ned. 50 prosent

av lederne er enig eller delvis enig at de som slutter blir slettet som bruker av IKT-systemet innen 14 dager, mens 36 prosent ikke har ansvar for det. I praksis overholdes ikke rutinen med å deaktivere brukere innen et bestemt tidspunkt etter at de har sluttet.

I spørreundersøkelsen oppgir 89 prosent at de er helt enig, enig eller delvis enig i at de bare har tilgang til programmer som er nødvendig for den stillingen de har.

Alle ansatte skal ha signert taushetserklæring. Det er 82 prosent av ansatte som oppgir at de har signert avtale om taushetsplikt. Sikkerhet vurderes å være mer personavhengig enn avhengig av passord. De fleste brukere er ifølge våre informanter, bevisstgjort på at de kan bli lurt.

I spørreundersøkelsen kommer det fram at 77 prosent av de ansatte aldri går fra PC-en med åpne programmer/dokumenter. 91 prosent oppbevarer ikke passord og brukernavn slik at andre kan finne det og 87,0 prosent låner aldri bort passord og brukernavn. Når det gjelder bytte av passord er det 74 prosent som skifter passord årlig eller sjeldnere og begrunnelsen er at de er redd for å glemme det.

Data i ASP-løsningen overføres til Evrys servere gjennom en egen kommunikasjons-løsning, egen VPN (virtual private network) forbindelse.

6.2.3 Sikring av integritet

Sikring av integritet innebærer at det skal være mulig å oppdage forsøk på uautorisert bruk av informasjonssystemet, at rettigheter til å endre data skal være knyttet til delegert myndighet og at sikkerhetstiltakene ikke skal være mulig å omgås av eller påvirkes av medarbeiderne. Kommunen arbeider med en sikkerhetsnorm og så langt er ikke sikkerhetstiltak dokumentert.

I referatet fra statusmøtet mellom kommunen og IT Partner 23.08.2016 framgår det at uautorisert bruk av IT-systemet er ikke oppdaget. IT-teknikeren antar at det finnes logger over dette i nettverket.

Dersom noen lokalt har foretatt en oppgradering, kan man se hvem som har gjort det. IT-teknikeren vet at dette gjøres, og han ønsker å ha full kontroll over slik aktivitet. IT-teknikeren er usikker på om alle endringer som gjøres kan spores.

Av referatet fra statusmøte mellom kommunen og IT Partner 23.08.2016 framgår det at IT Partner skal gi tilbud på et verktøy som heter ProAktiv for å visualisere Sømna kommunes IT-systemer på kontrolltavler i sitt kontrollmiljø. ProAktiv baserer seg på trafikklysprinsippet der de mest vitale parameter på tjenermaskiner og nettverks-infrastruktur overvåkes i sanntid. I tillegg til å være avgjørende for å varsle kritiske feil, loggføres avvik med tidspunkt og varighet for hendelsen. Systemet kan også generere visuelle rapporter over nettverkstrafikk, og på den måten gi full kontroll på

kommunens dataflyt. IT Partner oppgir at ProAktiv ikke vil medføre en endring i avtalen, men at fokus flyttes fra systemsjekk til en mer automatisert overvåkning.

6.2.4 Sikring av tilgjengelighet (sikring mot tap av data)

Sikring av tilgjengelighet betyr å oppfylle krav til service, slik at alle berettigede krav om tilgang til informasjon dekkes ved behov. Dette omfatter rutiner for backup og reserveløsninger for å ivareta kritiske data.

IT Partner har ansvar for backup. IT-teknikeren er kjent med at det tas backup hver natt, og leverandøren sjekker at backup er kjørt (fjernstyrt, ikke direkte på lokasjon). Backup oppbevares fysisk i huset, men noe sendes også til nettverksenhet på sykehjemmet.

Revisor har fått tilgang til rutinebeskrivelse for backup (gjelder backup av servere og tilhørende data). Sømna kommune benytter verktøyet Veeam for å håndtere backup av virtuelle servere, og komplett kopi av hver virtuell server lagres til eksternt NAS[5]. NAS'et er fysisk plassert i kjelleren på sykehjemmet. Videre benyttes Veeam Endpoint for å ta backup av fysisk windows maskin. Det gjennomføres komplett serverbackup daglig, med unntak av et par backuper som skjer ukentlig. All varsling fra backup går til IT Partner.

I systemsjekken som IT Partner gjør i form av kontroll av maskinvare, operativsystem og sikkerhetssystem, oppdages begynnende feilsituasjoner før de får konsekvenser for tilgjengeligheten av systemene. Kritiske parametere for stabil drift sjekkes til faste tider. Avvik fra anbefalingene dokumenteres og tiltak foreslås.

Dersom en fiberkabel ryker mister Sømna kommune internettbaserte program slik som programmene i ASP-løsningen. Kommunen har også vanlig bredbånd. Bredbåndslinja er til helsenett som brukes av legekontoret.

6.3 Vurdering

Internkontroll

Internkontroll skal være etablert og dokumentert og kommunens internkontroll på området skal vedlikeholdes. I dag ligger den gamle ROS-analysen fra 2013 i kvalitetssystemet Compilo og den er utdatert. Sømna kommune mangler en sikkerhetsnorm med mål og strategier for informasjonssikkerhet i kommunen. En slik sikkerhetsnorm er grunnlaget for kommunens internkontroll. Arbeidet med sikkerhetsnormen er igangsatt, men pr høsten 2017 er det lite framdrift i arbeidet.

[5] NAS: nettverkslagring

Kommunens internkontroll skal være kjent for medarbeiderne. Så lenge sikkerhetsnormen er under utarbeidelse så vil ikke ansatte kjenne til internkontroll som gjelder for IKT området.

Konfidensialitet

Dataenes konfidensialitet skal være sikret. Dette omfatter blant annet at det skal være etablert tiltak som hindrer uautorisert personell tilgang til sensitiv/gradert informasjon. Kommunen bruker nettverkssegmentering for å hindre at uautorisert personell ikke får tilgang til sensitive data/ gradert informasjon. Det skal være etablert et system for tilgangskontroll. Slik det fungerer i dag er det leder som bestemmer hvilke tilganger den enkelte ansatte skal ta. Det finnes ingen dokumentasjon eller retningslinjer for hvem som skal ha tilgang til hva. Det er naturlig at noen PCer i kommunen brukes av flere, for eksempel på vaktrom på sykehjemmet. Revisor har ingen informasjon om det finnes rutiner for flerbruker PCer.

Tilgangskontroll skal være tilpasset slik at bruker ikke gis tilgang til andre opplysninger enn vedkommende har bruk for i sin stilling. Grupper i AD (Active directory) styrer hvem som har tilgang til hva. Revisor har signaler på at det er behov for å gjennomgå hvem som har tilgang til hvilke mapper innenfor lege, psykiatri og helsestasjon.

Tildeling av passord bør styres av en formell administrasjonsprosess. Nyansatte får innføring i hvordan passord endres. Det skal være rutiner for endring av passord. Det tyder på at det er opp til den enkelte ansatte å endre passord når de fleste gjør dette årlig eller sjeldnere. Dette underbygger revisors oppfatning av at kommunen ikke har rutiner for endring av passord.

Det skal være etablert rutine for fjerning av tilganger for midlertidige brukertilganger og brukere som slutter. IT-teknikeren oppgir at tilganger deaktiveres med en gang, mens epost blir stående ca. en uke. Spørreundersøkelsen tyder på at dette ikke skjer hver gang og at rutinen ikke etterleves fullt ut.

Integritet

Dataenes integritet skal være sikret og det skal være mulig å oppdage forsøk på uautorisert bruk av informasjonssystemet. Gjennom logger er det mulig å kontrollere uautorisert bruk av datasystemet.

En del av integriteten er at rettigheter til å endre data skal være koblet til delegert myndighet. I praksis er mulighetene til å endre data knyttet til de tilgangene den enkelte har. Tilgangen bestemmes av lederne og hvis man ikke har retningslinjer for hvem som skal ha hvilke tilganger, så kan tildeling av tilganger bli tilfeldig. Bruken av gruppetilganger i AD (active directory) kan føre til at flere får tilganger de ikke burde hatt fordi de er definert inn i gruppen. IKT-systemet har logger over bruken, men revisor er av den oppfatning at retningslinjene bak hvem som skal ha hvilke rettigheter

knyttet til den delegerte myndigheten er mangelfull og inndeling i grupper for gruppetilgang innebærer en risiko for at andre også får tilgang.

Sikkerhetstiltakene skal ikke kunne påvirkes eller omgås av medarbeiderne. Sikkerhetstiltakene er ikke dokumentert. Når kommunen mangler retningslinjer for tildeling av tilganger, ut over at nærmeste leder bestiller tilganger, kan det være mulig at noen kan argumentere til å få tilganger som de kanskje ikke burde ha. Bruken av AD (active directory) styrer tilgangen teknisk, så den største muligheten til å omgås systemet er å få tillatelse til en tilgang som man ikke burde ha.

Tilgjengelighet

Dataenes tilgjengelighet skal være sikret gjennom at det er etablert backup-rutiner som sikrer tilgjengelighet av data og at det finnes reserveløsninger for kritiske data. Kommunen har backup rutiner som håndteres av IT Partner og det tas backup daglig. Kritiske data for helse og omsorgssektoren er tilgjengelig gjennom NAS (nettverkslagring) som er lokalisert i kjelleren på sykehjemmet.

7. KONKLUSJON

I dette prosjektet har vi vurdert i hvor stor grad har Sømna kommune sikret et godt styringssystem for IT gjennom å ivareta utvalgte styrings- og kontrollmål i anerkjent kvalitetsstandard (COBIT).

Et godt styringssystem skal være forretningsorientert og prosessorientert, basert på kontrolltiltak og på oppfølging av målbare parameter. Styringssystemet skal være en modell for å styre virksomhetens bruk av IT. Det er flere elementer som bidrar til at styringssystemet er en god modell for å styre virksomhetens bruk av IT. I dette prosjektet har innfallsvinkelen vært å se hvorvidt utvalgte styrings- og kontrollmål i COBIT er ivaretatt. Vi har vurdert styrings- og innenfor alle fire hovedområder:

1. Planlegging og organisering

- Sømna kommune har ingen IT/IKT-strategi son viser overordnede mål, veivalg knyttet til IKT og konkrete handlingsplaner. Kommunen er i ferd med å lage en digitaliseringsstrategi, som en sektorstrategi til samfunnsplanen, som er under utarbeidelse. Det er uklart om den planlagte digitaliseringsstrategien vil tilfredsstille kravene til en IKT-strategi.
- Ansvars- og myndighetsforholdene for bruk av IKT-systemet er lite dokumentert ut over det som framgår av kontrakter med IT Partner og ASP-avtalen med Evry, og lite kjent for organisasjonen.
- Kravet om hensiktsmessig og sikker sammenkobling av maskinvare og høyre sikkerhetsnivå for sensitive data er oppfylt, og konfigurasjonen er dokumentert.
- Sømna kommune har en utdatert ROS-analyse, men har en metodikk som det kan bygges videre på, blant annet kriterier for akseptabel risiko.

2. Anskaffelse og implementering

- Kommunen mangler kravspesifikasjon for anskaffelse av IKT.
- Kommunen mangler plan for investering og utskifting av maskinvare og programvare.
- Gjennom avtalen med IT Partner har kommunen og leverandører av spesifikk programvare tilgang på kompetent personell for installasjon og implementering av systemer.

3. Driftsleveranse og støtte

- I avtalen med IT Partner er responstid definert og i ASP-avtalen med Evry er oppetid og responstid definert.
- Opplæringen av brukere er mangelfull og spesielt dårlig er det på informasjonssikkerhet, slik at ansatte har lite kjennskap til retningslinjer og rutiner for informasjonssikkerhet.

- I avtalen med IT Partner og for intern help-desk er det etablert et system med registrering av feilmeldinger og et system for oppfølging.
- Det genereres aktivitetslogg som viser bruken av IKT-systemet, herunder uautorisert bruk.
- Sømna kommune har tilfredsstillende fysisk sikring av serverrom mot uautorisert adgang.

4. Kontrolltiltak

- Sømna kommune har ikke en vedlikeholdt internkontroll for IKT og dermed ikke en kjent internkontroll for medarbeiderne.
- Kommunen har det tekniske systemet for tildelinger av tilganger i IKT-systemet i orden og gjennom nettverkssegmentering ligger sensitive data på sikker sone. Leder bestemmer hva ansatte skal ha tilgang til og det mangler retningslinjer for hvem som skal ha tilgang til hva. Kommunen mangler rutiner for endring av passord.
- Tilgangssystemet gjennom AD (active directory) er en tilfredsstillende teknisk løsning for å sikre integriteten, men har ikke dokumentert sikkerhetstiltak og det mangler retningslinjer for hvem som skal ha tilgang ut over at leder bestemmer.
- Gjennom avtalen med IT Partner har kommunen backuprutiner som sikrer tilgjengelighet av data og det finnes en reserveløsning for kritiske data.

Hovedkonklusjon

På bakgrunn av disse vurderingene, konkluderer revisor med at Sømna kommune delvis har sikret et godt styringssystem for IT/IKT gjennom at utvalgte styrings- og kontrollmål i anerkjent kvalitetsstandard (COBIT) er ivaretatt.

8. ANBEFALINGER

På bakgrunn av vurderinger og konklusjon vil revisor anbefale:

- Kommunen bør sikre at digitaliseringsstrategi inneholder det som forventes av en IKT-strategi som viser overordnede mål og veivalg samt konkrete handlingsplaner, herunder en sikkerhetsnorm/strategi og en plan for investering og utskifting av maskinvare.
- Kommunen bør tydeliggjøre og dokumentere ansvar og myndighet innenfor IKT-området og herunder etablere rutiner for hvem som skal ta tilgang til hva.
- Kommunen bør utarbeid en internkontroll på IKT-området.
- Kommunen bør oppdatere ROS-analysen.

9. RÅDMANNENS KOMMENTARER

En foreløpig rapport ble sendt på høring til rådmannen i Sømna kommune 6. november 2017. KomRev Trøndelag IKS mottok svar fra rådmannen 21.november 2017. Høringssvaret er gjengitt under. Revisor har korrigert rapporten med oppdaterte opplysninger i tråd med tilbakemeldingene fra rådmannen. Høringssvaret har ut over dette ikke medført endringer i rapporten.

9.1 Høringssvar

Vi har gjennomgått høringsrapporten om IKT i Sømna.

Hovedinntrykket er at rapporten er god og gjennomarbeidet.
Rådmannen har følgende kommentarer:

- *I sammendraget bør det fremkomme at kommunen i den pågående organisasjonsgjennomgangen skal ha på plass en digitaliseringsansvarlig i stab. Dette vil nå komme på plass.*
- *Under revisjonskriterier, pkt 1.4, hadde det vært ønskelig med en henvisning til relevante styringsdokumenter for digitalisering i offentlig sektor, da disse legger føringer på kommunenes prioriteringer fremover. Aktuelle dokumenter kan være regjeringens stortingsmelding om digitalisering fra 2016 eller KS' digitaliseringsstrategi. Dette er viktig, da det trekkes konklusjoner om kommunens planer om digitaliseringsstrategi uten at revisjonskriteriene er klare på dette. Det er en tydelig mangel ved rapporten.*
- *I skissen over overordnet AD og nettverksdesign fremkommer noe sensitiv informasjon. Den må selvsagt slettes.*
- *Rådmannen er direkte uenig i vurderingen gjort i punkt 3.3. Kommunen må ha informasjonssikkerhet med i fremtidig digitaliseringsarbeid. På intervjutidspunkt var kommunens digitaliseringsutfordringer ikke fullt gjennomarbeidet. En intern GAP-analyse er nylig gjennomført og vil bidra til retning og struktur i digitaliseringsarbeidet.*

Jeg ser frem til presentasjonen av endelig rapport 5.12 og videre anledning til å komme med flere spørsmål og kommentarer til rapporten.

Mvh
Øystein Johannessen

Rådmann/Chief Executive
Sømna kommune

KILDER

Brønnøy kommune og Evry Norge AS 2015: Avtale om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare

Cobit (Control Objectives for Information and Related Technology)
Kvalitetsstandard for IKT

Datatilsynet (2009): En veileder om internkontroll og informasjonssikkerhet. Datatilsynet

Difi.no

ISACA (2013) Styringssystem for IKT – styrende dokumenter. 3. utg. ISACA Norway Chapter

IT Partner og Sømna kommune, 2015. Avtale om drift, vedlikehold og service av utstyr og programvare.

IT Partner: referat fra statusmøte 26. august 2016

IT Partner, referat fra statusmøte 21. november 2016

Lov om behandling av personopplysninger (personopplysningsloven) av 14.04.2000: Forskrift om behandling av personopplysninger (personopplysningsforskriften)

Sunde, S.J. (2006): Rammeverk for IT-styring i ny utgave: CobiT. Revisjon og regnskap, årg. 76, nr. 3, s.35-37

Sømna kommune. Delegasjonsreglement.
http://www.somna.kommune.no/www/somna/resource.nsf/files/wwww8ragwl-delegasjonsreglement/$FILE/delegasjonsreglement.pdf, 3. november 2017

Sømna kommune, Organisasjonskart.
http://www.somna.kommune.no/www/somna/resource.nsf/files/1536687355-organisasjonskart-sk-2016/$FILE/organisasjonskart-sk-2016.pdf, 3. november 2017.

Sømna kommune, høringsutkast 2.gangs høring kommuneplan for Sømna 2017-29.
http://www.somna.kommune.no/www/somna/resource.nsf/files/3411925725-hoeringsutkast_-_2-gangs_hoering_kommuneplanens_samfunnsdel_okt17/$FILE/hoeringsutkast_-_2-gangs_hoering_kommuneplanens_samfunnsdel_okt17.pdf

Sømna kommune. Plan for digitalisering. Sømna formannskap utv.saksnr. 72/17

VEDLEGG 1 REVISJONSKRITERIER

Revisjonskriterier er de krav og forventninger som kommunens praksis vurderes opp mot.

I dette prosjektet er kriteriene hentet fra:

- COBIT (Control objectives for Information and Related Technology), Kvalitetsstandard for IKT
- Personopplysningsloven med tilhørende forskrifter
- E-forvaltningsforskriften

COBIT er alene dekkende som kilde til revisjonskriterier. På enkelte områder innenfor informasjonssikkerhet har lovgiver har gått lengre, og vi benytter derfor også disse som kilder til kriterier.

I COBIT har man satt opp 34 overordnede styrings – og kontrollmål. Disse er fordelt på fire hovedområder:

- Planlegging og organisering
- Anskaffelse og implementering
- Leveranse og støtte
- Overvåking (kontrolltiltak)

Planlegging og organisering omhandler blant annet følgende styrings- og kontrollmål:

- Definere en IT-strategi i samsvar med kommunens overordnede mål.
- Utforme IT-organisasjonen og IT-prosessene
- Definere en informasjonsarkitektur
- Risikostyring

I Personopplysningsforskriften § 2-7 som handler om organisering, heter det blant annet at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Videre slås det fast at ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.

Personopplysningsforskriften § 2-7 bestemmer også at informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås, at konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder, og at bruk av informasjonssystemet som har betydning for informasjons-sikkerheten, skal utføres i henhold til fastlagte rutiner.

Risikovurdering omtales i personopplysningsforskriften § 2-4:

Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og § 2-2.

Resultatet av risikovurderingen skal dokumenteres.

Anskaffelse og implementering inneholder følgende styrings – og kontrollmål:

- Identifisere løsninger
- Anskaffelse og vedlikehold av applikasjoner
- Anskaffelse og vedlikehold av teknologisk infrastruktur
- Installasjon og godkjenning av systemer

I forbindelse med **driftsleveranse og støtte**, peker COBIT på at de er viktig å definere og styre servicenivået. Videre er brukeropplæring sentralt, for på denne måten å sikre at brukerne anvender teknologien på en effektiv måte og er klar over risiko og ansvar forbundet med det. Brukerstøtteregimet skal omfatte mottak for behandling av hendelser og håndtering av problemer og hendelser. Dette betyr at Brukerstøtte/help-desk skal sikre at problemene brukerne har blir løst på en god måte. Dette betyr eksempelvis at brukerstøtte skal være lett tilgjengelig og yte hjelp innen rimelig tid, og at problemer og hendelser blir tatt hånd om og at årsakene blir etterforsket for å hindre gjentakelse.

Håndtering av data er også omfattet av hovedområdet driftsleveranse og støtte. Personopplysningsforskriften § 2-8 har bestemmelser som sier at medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Videre skal medarbeiderne ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt, og autorisert bruk av informasjonssystemet skal registreres.

Fysiske omgivelser reguleres av personopplysningsforskriften § 2-10, som blant annet sier at det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her. Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten.

Overvåking handler om å at internkontroll er sentralt. E-forvaltningsforskriften § 15 har bestemmelser om internkontroll på informasjonssikkerhetsområdet:

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.

Også personopplysningsloven (§ 14) har bestemmelser om internkontroll; og sier blant annet:

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.

Styring og kontroll er et annet styrings- og kontrollmål. I COBIT pekes det på at kontrolltiltak kan deles i to hovedgrupper:

- Generelle kontrolltiltak
  - Systemutvikling
  - Endringshåndtering
  - Sikkerhet
  - Drift
- Applikasjonsmessige kontroller
  - Fullstendighet

- Nøyaktighet
- Gyldighet
- Autorisert
- Arbeidsdeling

Sikring av konfidensialitet reguleres i personopplysningsforskriften § 2-11, som blant annet sier at det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Samme forskrift § 2-12 omhandler sikring av tilgjengelighet gjennom bestemmelsen om at det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig. Bestemmelser om sikring av integritet er regulert i forskriftens §§ 2-13: Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Personopplysningsforskriften § 2-14 har bestemmelser om sikkerhetstiltak:

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Forsøk på uautorisert bruk av informasjonssystemet skal registreres. Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre. Sikkerhetstiltak skal dokumenteres.

På bakgrunn av disse kildene har vi utledet følgende kriterier:

Planlegging og organisering:

1. Kommunen skal ha en IT-strategi som
   - viser kommunens overordnede mål og hvordan IT skal bidra til å nå målene
   - viser veivalg knyttet til IT
   - viser konkrete handlingsplaner
2. Det skal etableres klare ansvars – og myndighetsforhold for bruk av informasjonssystemet
3. Ansvars – og myndighetsforhold skal være dokumentert
4. Endringer i ansvars – og myndighetsforhold skal godkjennes av øverste myndighet
5. Utstyr og program skal være sammenkoblet på en hensiktsmessig og sikker måte
6. Sensitive data skal ha høyere sikkerhetsnivå
7. Konfigurasjonen skal dokumenteres
8. Det skal gjennomføres og dokumenteres ROS-analyse for informasjons-sikkerhet
9. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger
10. ROS-analysen skal klarlegge sannsynlighet for og konsekvenser av sikkerhetsbrudd
11. Resultatet av risikovurderingene skal sammenlignes med de fastlagte kriteriene for akseptabel risiko forbundet med behandling av person-opplysninger
12. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten

Anskaffelse og implementering:

1. Kommunen bør ha utarbeidet en kravspesifikasjon til sin leverandør før anskaffelser innen IKT.
2. Kommunen bør ha en plan for investering og utskifting av maskinvare (pc, servere, utstyr til nettverk etc).
3. Kommunen bør ha en plan for investering i og vedlikehold av programvare, og sørge for at kommunens programvare til enhver tid er oppdatert.
4. Kommunen bør sørge for at installasjon og implementering av systemer utføres av kompetent personell.

Driftsleveranse og støtte:

1. Forventet servicenivå skal være definert i avtale med leverandør; herunder oppetid på systemet og responstid for bistand, rapportering fra leverandør
2. Brukere skal gis opplæring i bruk av systemet (alle funksjonaliteter i systemet)
3. Ansatte skal ha kjennskap til retningslinjer og rutiner for informasjons-sikkerhet
4. Det skal være etablert et system for registrering av feilmeldinger og hendelser
5. Systemet skal bidra til at innmeldte feilmeldinger og hendelser blir fulgt opp
6. Autorisert bruk av systemet skal dokumenters gjennom en aktivitetslogg
7. Serverrom skal være sikret fysisk mot uautorisert adgang

Kontrolltiltak:

1. Kommunens internkontroll(tiltak) på området skal vedlikeholdes
2. Kommunens internkontroll (tiltak) skal være kjent for medarbeiderne
3. Dataenes konfidensialitet skal være sikret:
    - Det skal være etablert tiltak som hindrer uautorisert personell tilgang til sensitiv/gradert informasjon
    - Det skal etableres et system for tilgangskontroll
    - Tilgangskontroll skal være tilpasset slik at bruker ikke gis tilgang til andre opplysninger enn vedkommende har bruk for i sin stilling
    - Tildeling av passord bør styres av en formell administrasjonsprosess
    - Det skal være rutiner for endring av passord
    - Det skal være etablert rutine for fjerning av tilganger for midlertidige brukertilganger og brukere som slutter
4. Dataenes integritet skal være sikret:
    - Det skal være mulig å oppdage forsøk på uautorisert bruk av informasjonssystemet
    - Rettigheter til å endre data skal være koblet til delegert myndighet
    - Tiltakene skal ikke kunne påvirkes eller omgås av medarbeiderne
5. Dataenes tilgjengelighet skal være sikret gjennom etablert backup rutiner og det skal være en reserveløsning for å ivareta kritiske data.

Postadresse: Postboks 2565, 7735 Steinkjer
Hovedkontor: Fylkets Hus, Steinkjer
Tlf. 994 01 480
www.krt.no