Rapport

Forvaltningsrevisjon – Informasjonssikkerhet og IT-drift

Oslo, 14. desember 2012

Rapporten er utarbeidet for oppdragsgiver, og dekker kun de formål som med denne er avtalt. All annen bruk og distribusjon skjer for oppdragsgivers regning og risiko. BDO vil ikke kunne gjøres ansvarlig ovenfor en tredjepart.

BDO

Innholdsfortegnelse

1. Sammendrag og forslag til tiltak

Kontrollutvalget i Vestby kommune har besluttet at det skal gjennomføres et forvaltningsrevisjonsprosjekt vedrørende informasjonssikkerhet og IT-drift. Formålet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard.

Hovedproblemstillingene for prosjektet har vært:

Tema: Informasjonssikkerhet
1. Har Vestby kommune tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
2. Tilfredsstiller Vestby kommune sikkerhetsbestemmelsene i personopplysningsforskriften?
Tema: IT-drift
3. Er det etablert overordnede mål, retningslinjer og rutiner for IT i Vestby kommune?
4. Følges god IT-skikk i Vestby kommune?
5. Er det tilfredsstillende arbeidsdeling vedrørende IT i Vestby kommune?
6. Har Vestby kommune rutiner for å gjenoppta normal drift etter driftsstans?
7. Har Vestby kommune rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?
8. Er maskinkapasiteten god nok for å sikre stabil drift?
9. Er kompatibiliteten mellom ulike datasystem i Vestby kommune tilfredsstillende?

1.1. Oppsummering

Informasjonssikkerhet og drift av IT-systemene synes å være godt ivaretatt innenfor flere av de belyste problemstillingene, og i henhold til god IT-skikk. Dette gjelder spesielt innefor ansvarsdeling og oppfølging av tjenesteleveranser, samt håndtering av endringer. Mål og strategier for IT i kommunen er dokumentert, og det er opprettet et styringssystem for informasjonssikkerhet som omhandler helsesystemer. Kommunen har også igangsatt et arbeid med etablering av et styringssystem for informasjonssikkerhet som omfatter alle systemer.

Kommunen bruker i liten grad en strukturert, risikobasert tilnærming for å identifisere tiltak som skal bidra til å sikre at styring og kontroll av IT er innenfor et definert, akseptabelt risikonivå. Beskrivelse og forankring av ansvar og plikter i rollen som systemeier er mangelfull, samt at prioriteringer av IT-systemer i eventuelle kontinuitets- og katastrofesituasjoner er noe uklart.

Dette medfører at flere sentrale forhold ved sikkerhetsbestemmelsene i personopplysningsforkriften ikke etterleves i tilstrekkelig grad. Videre har revisjonen avdekket at flere viktige emner innenfor de aktuelle problemstillingene, kontinuitets og katastrofeplaner spesielt, bør forbedres.

Denne rapporten omhandler svært mange problemstillinger, tildels overlappende, som både hver for seg og i sum er omfattende og komplekse for en overordnet gjennomgang slik som denne revisjonen. Mottatt høringsuttalelse peker også på at presisjonsnivået på observasjoner og konklusjoner varierer mellom problemstillingene, hvilket er tilfelle gitt vår egen risikovurdering av hva som bør vektlegges og prioriteres for å gi et tilstrekkelig bilde av overordnet styring og kontroll med IT-drift og informasjonssikkerhet i Vestby kommune innenfor prosjektets rammer og ressurstilgang.

Vi deler rådmannens syn på at det ikke er noen forhold som bør fremkalle vesentlige bekymringer for IKT i Vestby kommune, men at det er enkelte områder som må eller bør forbedres.

1.2. Problemstilling #1 – Rutiner og retningslinjer for informasjonssikkerhet

Har Vestby kommune tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?

Resultatområdene har for de fleste av sine IT-systemer inngått tjenesteavtaler som omfatter tilgjengelighet.

Med unntak av helsesystemene, omhandlet i dokumentet "Personvern og informasjonssikkerhet for Vestby kommune", er det ikke kommunisert retningslinjer og føringer for enhetlig klassifisering av de øvrige IT-systemene og for lagret informasjon i lys av konfidensialitet, integritet og tilgjengelighet.

Dette kan medføre at risikoer i kritiske systemer ikke blir identifisert og ivaretatt med tilstrekkelige rutiner og kontroller.

1.3. Problemstilling #2 – Etterlevelse av sikkerhetsbestemmelsene i personopplysningsforskriften

Tilfredsstiller Vestby kommune sikkerhetsbestemmelsene i personopplysningsforskriften?

Forskriften pålegger databehandler en risikobasert tilnærning i sitt arbeid med informasjonssikkerhet. IKT-avdelingen utfører risikovurderinger av sine tjenester og kommuniserer til kommunens ledelse behov for investeringer i tekniske sikkerhetstiltak. Kommunen mangler imidlertid klare retningslinjer for klassifisering av IT-systemer. Slik klassifisering er avgjørende for å kunne sikre en helhetlig vurdering og prioritering av risikoreduserende tiltak og målrettede investeringer.

Dette medfører risiko for at sikkerhetsarbeidet blir ad-hoc preget og ikke helhetlig risikotilnærming som er i harmoni med kommunens sikkerhetsmål og risikoappetitt.

1.4. Problemstilling #3 – Overordnede mål, retningslinjer og rutiner for IT

Er det etablert overordnede mål, retningslinjer og rutiner for IT i Vestby kommune?

Kommunen har definert mål, strategier og retningslinjer for IKT i kommunen. Planen mangler imidlertid kriterier for klassifisering av informasjon og systemer. Akseptabel risiko omhandler kun helsesystemer. De styrende dokumentene benytter ulike beskrivelser av roller og ansvar for organisering av informasjonssikkerhetsarbeidet. Prioritering av IT prosjekter kommer ikke frem av IT-planen.

Dette kan medføre at informasjonssikkerheten ikke blir tilstrekkelig ivaretatt ved at:

- IT-systemer hverken forvaltes eller opererer innenfor akseptabel risiko
- Kritiske IT-prosjekter får ikke riktig prioritet
- Beskrivelser av roller og ansvar gir høy grad av tolking og preges av personlige preferanser
- Uklart ansvar for oppfølging av kommunenes etterlevelse av lover og forskrifter

1.5. Problemstilling #4 – Vestby kommunes etterlevelse av god IT-skikk

Følger Vestby Kommune god IT-skikk?

Vestby kommune følger flere av retningslinjene gitt for god IT-skikk.

Kommunen mangler imidlertid retningslinjer for klassifisering av verdier samt fastsettelse av akseptabel risiko. Slik klassifisering er avgjørende for tilstrekkelig å kunne sikre en helhetlig vurdering og prioritering av systemer og behov for etablering av risikoreduserende tiltak som igjen sikrer målrettede investeringer.

Ansvaret som ligger i rollen som systemeier er uklart presisert, og dette medfører at utøvelse av rollen ikke blir enhetlig, men preges av personlige preferanser.

Kontinuitetsplanene for IKT mangler knytning mot kommunens beredskapsplaner mtp å sikre prosesser som har størst prioritet. Dette kan medføre at kontinuitets- og katastrofeplaner for IT-systemene ikke understøtter kommunens kritiske prosesser.

1.6. Problemstilling #5 – Tilfredsstillende arbeidsdeling vedrørende IT

Er det tilfredsstillende arbeidsdeling vedrørende IT i Vestby kommune?

Arbeidsdelingen vedr. drift og forvaltning av IT i Vestby kommune, synes å være tilfredsstillende.

Det er rom for nærmere avklaring og dokumentasjon av ansvaret som hviler på systemeier i lys av risiko, herunder etablering av tiltak samt å sikre etterlevelse av lover og forskrifter.

1.7. Problemstilling #6 – Rutiner for reetablering av IKT-tjenester etter driftsstans

Har Vestby kommune rutiner for å gjenoppta normal drift etter driftsstans?

Det ble i 2009 igangsatt en utredning med sikte på å utrede kommunenes behov ved en eventuell katastrofe eller ved driftsstans. Det ble dog ikke utarbeidet helhetlige katastrofeplaner etter dette som berører IT. I de katastrofetestene som har blitt gjennomført så har IT kun vært involvert for å sikre telefoni.

IT har selv utarbeidet planer for de mest kritiske systemene innen helse, personal og sak/arkiv. Det er imidlertid ikke utarbeidet en helhetlig dokumentert plan som er i samsvar med kommunes katastrofeplan.

1.8. Problemstilling #7 – Rutiner for endringshåndtering innen IT

Har Vestby kommune rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?

Det er IKT-rådene og styringsgruppen som tar avgjørelsen om prioritering av prosjekter. Ved større endringer opprettes en prosjektgruppe. Endringer utføres og testes etter en fastsatt sjekkliste/arbeidsplan som dokumenteres i sakssystemet. Det gjøres ingen klassifisering av endringer, men standardendringer (dvs. endringer som IKT kan gjøre uten å starte et prosjekt) er spesifisert i SLA som IKT har med RO-ene.

Kommunen synes å ha etablert en prosess som sikrer tilfredsstillende kontroll med endringer i IT-systemene.

1.9. Problemstilling #8 – Overvåking av kritiske systemressurser

Er maskinkapasiteten god nok for å sikre stabil drift?
Revisjonen har ikke funnet forhold som tilsier Vestby kommune ikke har rutiner for overvåkning og oppfølging av kritiske systemressurser.

1.10. Problemstilling #9- kompatibilitet mellom ulike datasystem

Er kompatibiliteten mellom ulike datasystem i Vestby kommune tilfredsstillende?
Samme informasjon lagres i flere datasystemer. Dette fordrer manuelle handlinger for å sikre tilstrekkelig datakvalitet og er krevende. Mangel på prosedyrer for vedlikehold av denne informasjonen medfører risiko for at integritet og konsistens i lagrede data ikke blir tilstrekkelig ivaretatt.

1.11. Forslag til tiltak

Det er ikke gjort funn som avdekker at rutinene og prosedyrene har vesentlige svakheter for de gjennomgåtte problemstillingene utover manglende kontinuitets- og katastrofeplanen for IT - kun mindre forhold påpekes utover dette. Det gis følgende forslag til tiltak:

Pkt	Forslag til tiltak
1	<u>Bedre katastrofeplanlegging</u> IKT bør harmonisere sin kontinuitets- og katastrofeplan med kommunens, slik at den understøtter kommunens behov og mål, særlig vedrørende nedetid og tap av lagret informasjon. Planen bør videre testes jevnlig og inkludere tjenestene som er utkontraktert til Follo-IKT.
2	<u>Bedre risikoplanlegging og risikostyring av systemer</u> Kommunens ledelse bør definere akseptabel risiko innenfor konfidensialitet, integritet og tilgjengelighet for alle IT-prosesser og -tjenester. Dette vil sikre en enhetlig klassifisering og prioritering av prosesser og IT-systemer, og er avgjørende i arbeidet med å identifisere behov for risikoreduserende tiltak. Det bør gjennomføres regelmessige risikovurderinger av kommunens systemer og prosesser. Dette vil avdekke mulige sårbarheter og avklare behov for risikoreduserende tiltak i lys av kommunens risikoappetitt og forpliktelser i lover og forskrifter. Etablerte tiltak bør overvåkes regelmessig for å sikre kontinuerlig forbedring og at kontrolltiltakene bidrar til at risikoen reduseres til eller beholdes på ønsket nivå.

Pkt	Forslag til tiltak
3	Bedre avklaring av roller og ansvar Systemeierrollen og ansvar knyttet til informasjonssikkerhet, bør presiseres og harmoniseres mellom de styrende dokumentene. Systemeier bør være ansvarlig for klassifisering av systemet med tanke på tilgjengelighet, integritet og kontinuitet. Systemeier bør sørge for at det er implementert tilstrekkelig tilgangkontroll for systemet i tråd med virksomhetens generelle regler, og er ansvarlig for å påse at det føres kontroll med tilganger i systemet gjennom regelmessig gjennomgang/revisjon. Dette sikrer at kun autoriserte brukere har tilgang og at tilganger er gitt i henhold til tjenestelig behov. Systemeieren bør i tillegg sørge for at nødvendige kontroller er innebygget i systemet/prosessen, som for eksempel sporbarhet, etterprøvbarhet, og at integriteten i designet blir ivaretatt. Rollen som informasjonssikkerhetsleder bør presiseres, og bør prinsipielt plasseres et sted i organisasjonen som ikke utfordrer habilitet. Kommunene bør etablere tiltak som sikrer at tildelte autorisasjoner blir regelmessig verifisert, at tildelt autorisasjon har en eier, og at eier av autorisasjonen er kjent med sitt ansvar og sine plikter.
4	Bedre oppfølging av sikkerhetstiltak Kommunen bør gjennomgå sine etablerte rutiner for arkivering av dokumentasjon med betydning for informasjonssikkerheten (passordregler, logger, osv). I tillegg til tekniske sikkerhetstiltak, omfatter dette også rutiner for arbeid med informasjonssystemet og registrering av hendelser. Slike rutiner bør arkiveres systematisk og i henhold til kravene i personopplysningsforskriften § 2.16. Lagringstid er 5 år fra det tidspunkt dokumentet ble tatt ut av bruk, eller fra tidspunktet for registrering av en hendelse. For hendelsesregistre gjelder en lagringstid på 3 måneder. For å sikre en strukturert verifisering av regelsett i brannmurer og andre barrierer, bør grunnkonfigurasjon av regelsettet dokumenteres (baseline). Først da kan avvik i gjeldene regelsett avdekkes systematisk. Slik dokumentasjon er i tillegg påkrevd i personopplysningsforskriftens § 2.14.
5	Bedre koordinering av systembehov Det bør ved innkjøp av nye systemer stilles krav for integrasjon med andre systemer, også fremtidig integrasjon hvor dette kan tenkes å være aktuelt. Dette bør klargjøres så tidlig som mulig i et prosjekt, samt opprette og legge til rette for vedlikehold av en data dictionary.

2. Formål og avgrensning

2.1. Bakgrunn og formål

Kontrollutvalget i Vestby kommune besluttet gjennomføring av et forvaltningsrevisjonsprosjekt vedrørende informasjonssikkerhet og IT-drift. Formålet med revisjonen ble satt til å belyse og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard.

Rapporten viser vår vurdering av kommunens håndtering av informasjonssikkerhet og IT-drift i henhold til problemstillingene, og gis en konklusjon for hver problemstilling. I sammendraget i kapittel 1 er det også gitt anbefalinger til tiltak.

2.2. Problemstillinger og revisjonskriterier

2.2.1. Problemstillinger

Kontrollutvalget har vedtatt følgende problemstillinger:

Tema: Informasjonssikkerhet
1. Har Vestby kommune tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
2. Tilfredsstiller Vestby kommune sikkerhetsbestemmelsene i personopplysningsforskriften?
Tema: IT-drift
3. Er det etablert overordnede mål, retningslinjer og rutiner for IT i Vestby kommune?
4. Følges god IT-skikk i Vestby kommune?
5. Er det tilfredsstillende arbeidsdeling vedrørende IT i Vestby kommune?
6. Har Vestby kommune rutiner for å gjenoppta normal drift etter driftsstans?
7. Har Vestby kommune rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?
8. Er maskinkapasiteten god nok for å sikre stabil drift?
9. Er kompatibiliteten mellom ulike datasystem i Vestby kommune tilfredsstillende?

Figur: Problemstillinger

2.2.2. Revisjonskriterier

Revisjonskriterier er kilder som er normgivende eller styrende for de spørsmål som vurderes. Det kan være lover og forskrifter, reglementer og instrukser, normer og standarder for yrkesutøvelse, vedtak osv. I dette prosjektet er det nettopp etterlevelse av regler som er formålet, og kriteriene som problemstillingene ble målt opp imot i dette prosjektet var:

- POL – Personopplysningsloven
- POF – Personopplysningsforskriften
- ISO 27001 – standarden ISO/IEC 27001:2005 ”Information security management systems - Requirements”
- ISO 27002 – standarden ISO/IEC 27002:2005 “Code of practice for information security management”
- COBIT - anerkjent rammeverk for styring og kontroll av IT, utgitt av profesjonsorganisasjonen ISACA
  - PO – hovedområdet ”Plan and Organise” – planlegge og organisere
  - AI – hovedområdet ”Aquire and Implement” – anskaffe og implementere
  - DS – hovedområdet ”Deliver and Support” – levere og støtte
- GITS – Serien Godt IT-skikk, utgitt av ISACA Norge

Revisjonskriteriene er knyttet opp mot problemstillingene i forhold til den enkelte sak, der disse har vært aktuelle å benytte som målestokk.

2.3. Metode og gjennomføring

Forvaltningsrevisjonen ble gjennomført i henhold til krav fastsatt i kommuneloven § 78, forskrift om revisjon i kommuner og fylkeskommuner og RSK 001 Standard for forvaltningsrevisjon (endringer per 1.2.2011). Den metodiske tilnærmingen skjedde i all hovedsak gjennom innhenting av data og gjennom intervjuer med aktuelle personer i kommunen.

Forvaltningsrevisjonen har primært bestått av intervjuer med:

Rune Sletner	Personal- og organisasjonssjef/IKT-sjef
Raymond Orderud	IKT-fagansvarlig
Rolf Sigurd Enger	Personalkonsulent

I tillegg er følgende personer fra de forskjellige resultatområdene (RO):

Kari Røen	Leder Fellestjenesten
Berit Sæbø	Arkivansvarlig
Sjur Authen	Økonomisjef
Hilde Hultin	IT-rådgiver Skole - Systemansvarlig
Liss Edvardsen	Systemansvarlig Helse Gerica.
Kristin Vestby	Ny leder for Arkiv
Grethe Hagbø	Ansvarlig Geodata og kartintegrasjoner (geodatasjef)
Hans Christian Fæste	RO-leder Plan, bygg og geodata
Vida Kvilhaugsvik	Superbruker og administrator/brukerstøte på Geodata - KomTek

Våre vurderinger og konklusjoner bygger på informasjon fra intervjuene samt mottatt dokumentasjon fra kommunen:

- 2010.10.19__serviceavtale pbg_ad. serviceavtaler.pdf
- 20120821 AGRESSO FOLLO STYRINGSGRUPPE agenda og vedtak.docx
- Applikasjons_oversikt_rs_v02.pdf
- Avtale Vestby kommune its.pdf
- IT-plan 2011-2014 inklusivt budsjettinput for 2011v1.doc
- Katastrofe-_og_datasikkerhetsutredning_v2.docx
- katastrofeplan presentasjon _ROledermøtet.ppt
- Katastrofeplan status per app.pdf
- MAL-Proskjektdefinisjon.pdf
- Organisasjonskart.pdf
- Overordnet-Systemkart.pdf
- Personvern og informasjonssikkehet_helse.docx
- prosjektdefinisjon eLink.pdf
- Prosjektdefinisjon Innføre PPS v2.pdf
- SLA-Gerica.pdf
- SLA-InfrastrukturTjenester-Eiendom.pdf
- SLA-Infrastrukturtjenester-PBG.pdf
- SLA-Lydia.pdf
- Utkast_Plan for informasjonssikring_Vestby_sep 12.docx

I tilknytning til vurderingene er det visuelt brukt symboler. Disse gir uttrykk for vår subjektive oppfatning av kvalitet i rutiner og intern kontroll i vurderingene. Symbolene representerer ikke en garanti for den reelle kvaliteten i rutinene og saksoppfølgingen. Vurderingene er basert på innhentet informasjon, og det vil alltid være en risiko for at forhold som ikke er omfattet av revisjonen, kunne ha medført en annen konklusjon.

Symbolbruken og beskrivelsen av denne er slik:

Symbol	Vurdering av kvalitet
Rød	**Kvaliteten må forbedres** – Det analyserte forholdet møter ikke den forventede standard eller krav i forhold til målekriteriene.
Gul	**Kvaliteten bør forbedres** – Det analyserte forholdet møter ikke alle aksepterte standarder eller krav i forhold til målekriteriene.
Grønn	**Kvaliteten er tilfredsstillende** – Det analyserte forholdet møter de fleste aksepterte standarder og krav.

Figur: Visualisering av subjektiv oppfatning av kvalitet

2.4. Avgrensning og begrensninger

Analyser, vurderinger, konklusjoner og forslag til tiltak bygger på den informasjonen som er mottatt. Gjennom høringen vil faktabeskrivelsen bli verifisert, men det kan fortsatt være opplysninger som av ulike grunner ikke har blitt forelagt, og som kunne gi andre vurderinger og konklusjoner enn det rapporten bygger på. Vårt arbeid er gjennomført innenfor en begrenset tidsramme og tidsperiode, og omfanget og fullstendigheten av analysene som er foretatt, må ses i lys av dette. Vi kan ikke gå god for at alle relevante forhold er avdekket eller analysert.

Verifisering av faktisk implementering av eksempelvis sikkerhet i infrastruktur, kontinuitetsløsninger, tilgangsnivåer og arbeidsdeling i applikasjoner er ikke omfattet av dette revisjonsprosjektet.

Rapporten viser vår vurdering av kommunens håndtering av informasjonssikkerhet og IT-drift i henhold til problemstillingene, og gis en konklusjon for hver problemstilling. I sammendraget i kapittel 1 er det også gitt anbefalinger til tiltak.

Verifisering av faktisk implementering av eksempelvis sikkerhet i infrastruktur, kontinuitetsløsninger, tilgangsnivåer og arbeidsdeling i applikasjoner er ikke omfattet av dette revisjonsprosjektet.

3. Om IKT-virksomheten i Vestby kommune

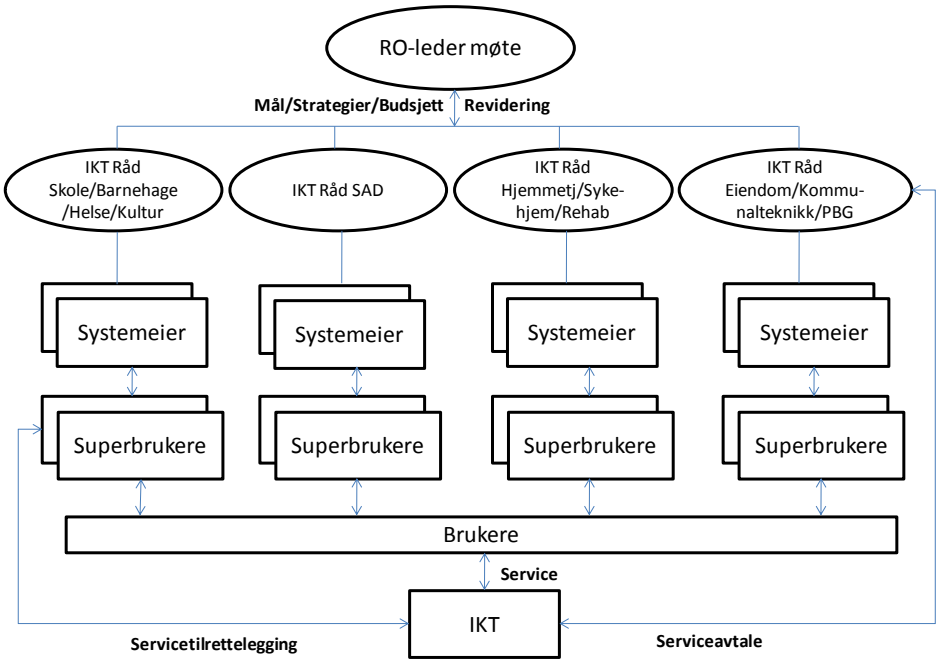
Her gis en overordnet oversikt og kort beskrivelse av IKT-virksomheten i Vestby kommune. Dette inkluderer IT-strategi, styrings- og organiseringsmodellen, samt en overordnet skisse over IKT-miljøet.

3.1. IKT-strategi

De overordnede målene for IKT i Vestby kommune skal nås gjennom å:

- Raskest mulig investere tilstrekkelig i IT-infrastruktur til å oppnå en enhetlig og stabil grunnmur med tilstrekkelig kapasitet
- Gjennomføre fornyelser innen applikasjonsporteføljen som bølger: Dvs. først sikre stabilitet og feilfrihet i alle applikasjoner for deretter planmessig å gjennomføre oppgraderinger og forbedringer i strukturerte prosjektprosesser ut fra kost/nytte vurderinger.
- I størst mulig grad bygge egen kompetanse i forvaltningen av IT-miljøet. Dvs. at gjennomføring i egen regi prioriteres fremfor rask fremdrift med innleide ressurser.

3.2. Styrings- og organiseringsmodell



Figur: Styrings- og organiseringsmodell

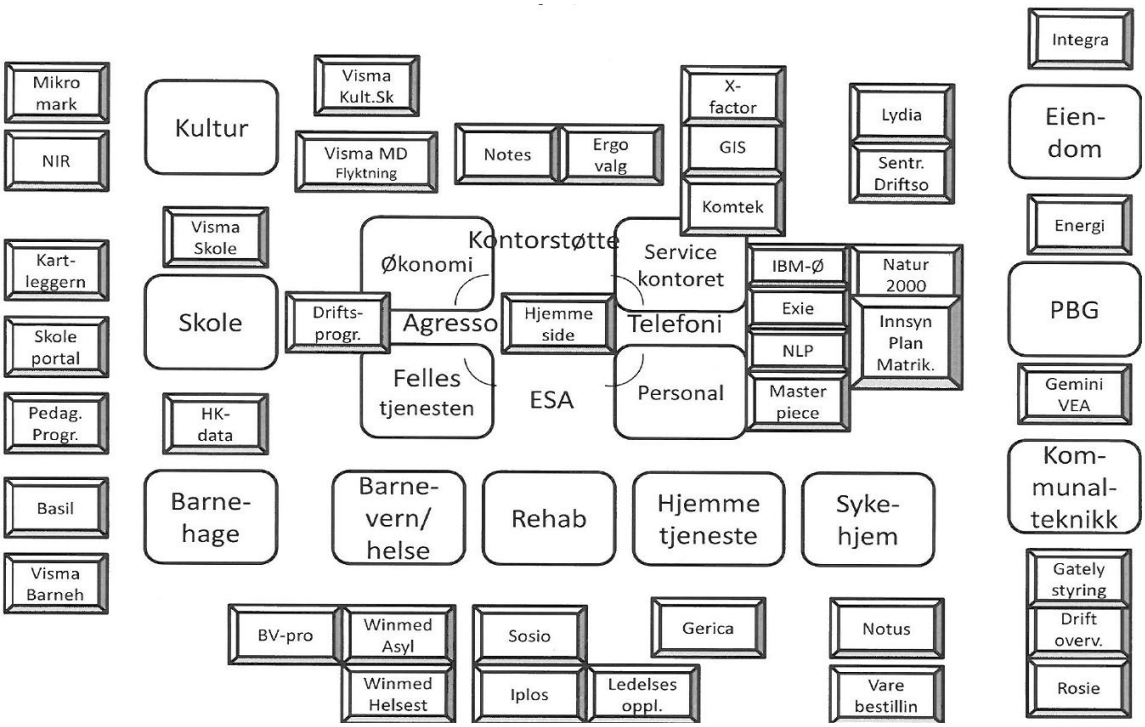
Følgende prinsipper gjelder for styrings- og organiseringsmodellen:

- RO-ledermøtet definerer rammene (mål, strategier, budsjett) for neste periodes arbeid med IKT og Telefoni på bakgrunn av en årlig IT-plan inklusivt budsjettforslag fra IKT-rådene.
- Personalsjefen er ansvarlig for å sammenstille den årlige IT-planen samt revideringene av denne.
- Det enkelte IKT-råd er ansvarlig for å målsette systemstøtten for arbeidsprosessene. De er også ansvarlig for å følge med på kvaliteten og kostnadseffektiviteten for det enkelte system som er underlagt rådet.
- IKT-avdelingen er selve service-utføreren i organiseringen av IKT og Telefoni i Vestby kommune.
- IKT-fagansvarlig er en nøkkelperson i både planlegging og utføring av IKT/Telefoniarbeide i Vestby. Dette betyr at selv om noen funksjonsområder har egne kompetente IKT-

medarbeidere, så skal IKT-fagansvarlig fungere koordinerende både under planlegging og utførelse av IKT-arbeid.

- IKT-fagansvarlig er ansvarlig for periodisk å avrapportere skriftlig til IT-rådet om - servicenivået siste periode. Hvor ofte dette er tjenlig avtales i IT-rådet.

3.3. Overordnet systemkart



Figur: Overordnet systemkart

Forvaltningen av systemene skal gjennomføres planmessig slik at både stabilitet/kvalitet ved innføring/endringer er akseptabel og kostnadsmessig er minst like gunstig som i snitt hos andre kommuner. Valget av å gjennomføre en oppgradering til ny versjon skal gjøres ut fra et skriftlig beslutningsunderlag hvor kost/nytte er styrende for beslutningen, og beslutninger om nye integrasjoner mellom applikasjoner gjøren kun etter en skriftlig utredning av konsekvenser for drift, stabilitet og påvirkning av kompleksiteten ved kommende vedlikehold og oppgradering av den totale applikasjonsporteføljen.

Alle systemer skal ha en systemeier som skal ha helhetsforståelse for både mål, funksjonalitet og bruk av systemet den er systemeier for. Den er normalt en del av ledelsen eller sitter nært ledelsen. Det skal også være tilknyttet superbrukere til systemene, som skal ha en dypere kunnskap om både funksjonaliteten til systemet den er superbruker for og den faktiske bruken av systemet i Vestby kommune.

4. Problemstilling #1 – Rutiner og retningslinjer for informasjonssikkerhet

4.1. Gjennomgang av problemstilling

Kommunens behandling av personopplysninger er underlagt kravene i personopplysningsforskriften (POF) som pålegger databehandleren at det etableres retningslinjer og rutiner som sikrer konfidensialitet, integritet og tilgjengelighet i behandlingen av personopplysninger.

Tabellen nedenfor viser våre funn og vurderinger fra vår gjennomgang:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #1: **Har Vestby kommune tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?**		
1	<u>Samlet oversikt over verdier/aktiva (Prosesser, informasjon og IT-systemer).</u> Flere av kommunens prosesser er avhengig av IT-systemer. Det bør derfor vedlikeholdes en samlet oversikt over dette der sammenheng og avhengigheter fremkommer. Kommunen har utarbeidet en oversikt over applikasjoner, men prosesser er ikke med i oversikten.	Grønn
2	<u>Eierskap til IT-systemene</u> Eierskap til applikasjoner(verdiene) er i hovedsak tildelt RO-ledere. Hvilke ansvar som ligger i rollen er beskrevet i *IT-planen* og *Personvern og informasjonssikkerhet for Vestby kommune (*videre kalt i *Styringssystemet for informasjonssikkerhet*). I sistnevnte er *Daglig ansvarlig* og *Systemansvarlig* gitt konkrete oppgaver for bl.a. tilgangskontroll og oppfølging av sikkerhetsarbeidet. I IT-planen synes ansvaret til systemeier å være lite presist og introduserer risiko for at utøvelse av rollen kan bli farget av personlige referanser og fokus.	Gul
3	<u>Klassifisering</u> Riktig klassifisering av prosesser/tjenester og systemer innenfor integritet, tilgjengelighet og konfidensialitet, danner grunnlaget for prioritering av systemer. I kommunens IT-plan finnes oversikter over de forskjellige systemene som benyttes av de forskjellige resultatområdene. Akseptabel risiko er definert i styringssystemet for informasjonssikkerhet (*Personvern og informasjonssikkerhet for Vestby kommune*), men dette omfatter kun helsesystemene. IT-planen gir ingen retningslinjer for klassifisering av de øvrige prosessene og IT-systemene innfor integritet, tilgjengelighet og konfidensialitet. En dokumentert prioritering av systemer er ikke utarbeidet. Men helsesystemer, personal og sak/arkiv(ESA) er de viktigste sentrale systemene etterfulgt av plan og bygningsetatens systemer og skolesystemene.	Gul

4	Akseptabelt risiko Akseptabelt risikonivå er beskrevet i styringssystemet for informasjonssikkerhet (*Personvern og informasjonssikkerhet for Vestby kommune*). Men dette omfatter kun helsesystemene og ikke de øvrige systemene/prosessene i kommunen.	Gul
5	Risikovurderinger Revisjonen har identifisert risikovurderinger for tilgjengelighet, da i relasjon til katastrofeplaner. For helsesystemer er det ikke utført risikovurderinger, men dette er planlagt utført i 2013. Risikovurderinger for andre systemer gjøres men dokumenteres i liten grad. Dette kan hindre en helhetlig oppfølging av arbeidet med informasjonssikkerhet, herunder identifisering av behov for tiltak som sikrer at systemene operer på akseptabelt risikonivå, og som er i harmoni med kommunens mål.	Rød
6	Oppfølging av risikoreduserende tiltak. Risikoreduserende tiltak er i hovedsak knyttet til gjennomgang av brukere, sjekk av backup, regler i brannmuren, OS-rettelser, ytelsesmålinger på samband og maskinpark og lignende. Sett i lys av mangelfulle risikovurderinger påvirker dette en systematisk og fullstendig oppfølging av etablerte tiltak – om de er effektive og reduserer risiko.	Gul

4.2. Vår konklusjon – Rutiner og retningslinjer for informasjonssikkerhet

Konklusjon: Har Vestby kommune tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?

Resultatområdene har for de fleste av sine IT-systemer inngått tjenesteavtaler som omfatter tilgjengelighet.

Med unntak av helsesystemene, omhandlet i dokumentet "Personvern og informasjonssikkerhet for Vestby kommune", er det ikke kommunisert retningslinjer og føringer for enhetlig klassifisering av de øvrige IT-systemene og for lagret informasjon i lys av konfidensialitet, integritet og tilgjengelighet.

Dette kan medføre at risikoer i kritiske systemer ikke blir identifisert og ivaretatt med tilstrekkelige rutiner og kontroller.

5. Problemstilling #2 – Etterlevelse av sikkerhetsbestemmelsene i forskriften

5.1. Gjennomgang av problemstilling

Personopplysningsloven (POL) § 13 og § 14 pålegger kommunen, ved kommunenes ledelse, å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger samt etablere systematiske tiltak for behandling av personopplysninger.

Dette er også en forutsetning for deltakelse i den elektroniske samhandlingsreformen – ref *"Veileder i organisering av samarbeid mellom helseforetak og kommuner om elektronisk samhandling"* og *"Norm for informasjonssikkerhet i helse- og sosialsektoren"*.

I tillegg til å identifisere sine plikter må kommunen tilpasse sin internkontroll og informasjons-sikkerhetstiltak til sin situasjon. Det samme gjelder for vedlikehold av internkontrollen hvor kommunen må tilpasse kontrollrutinene slik at rutiner og tiltak gjenspeiler behovene over tid.

Personopplysningsforskriften (POF) § 2 og § 3 definerer nærmere hvilke krav som hviler på kommunen, for at sikre tilfredsstillende informasjonssikkerhet. Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av kravene:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #2: Tilfredsstiller Vestby kommune sikkerhetsbestemmelsene i personopplysningsforskriften?		
1	§ 2.3 - Sikkerhetsledelse Kommunen har utarbeidet sikkerhetsmål og strategi som omfatter beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Disse er imidlertid ikke evaluering siste år, men det er et pågående arbeid med å oppdatere sikkerhetsmål og strategier. Strategi for datasikkerhet omhandler katastrofeløsninger og tekniske løsninger som brannmur-løsninger og virusforsvar mot eksterne trusler. Annen strategi vedrørende konfidensialitet, tilgjengelighet og integritet omhandles i mindre grad.	Grønn
2	§ 2.4 – Risikovurdering Kommunen har en oversikt over IT-systemene som inneholder personopplysninger. Systemene er tildelt systemeiere. Det finnes imidlertid få retningslinjer for klassifisering, med unntak av helsesystemene. Dette medfører risiko for at klassifiseringen ikke blir helhetlig. Kommunen gjennomfører risikovurderinger, men disse dokumenteres i liten grad. Vurderinger av sikkerhet i datanettverkets konfigurasjon og hvilke risikoer som denne introduserer relatert til innsyn i informasjon lagret i katalogtjenesten, er f.eks. ikke kjent for revisjonen. Mangelfull helhetlig tilnærming til risiko kan hindre en effektiv oppfølging av arbeidet med informasjonssikkerhet. En helhetlig tilnærming vil sørge for identifisering av behov for tiltak som sikrer at systemene gjennom målrettede investeringer, opererer på akseptabelt risikonivå og er i harmoni med kommunens sikkerhetsmål.	Gul

Pkt	Fakta og vurderinger	Kvalitet
3	§ 2.5 – Sikkerhetsrevisjon Det er implementert en rekke sikkerhetstiltak for beskyttelse av helseopplysninger som skal sikre kontroll med tilgang, konfidensialitet og integritet. Men det gjøres i liten grad regelmessig verifikasjon på at etablerte tiltak er operative og konsistente. Mangelfull strukturert oppfølging av etablerte sikkerhetstiltak medfører at kommunen ikke klarer å fange opp om etablerte tiltak fungerer som tiltenkt. Dette medfører risiko for at IT-systemene og lagret informasjon ikke opererer på akseptabelt risikonivå.	Gul
4	§ 2.6 - Avviksbehandling Kommunen har mangelfull rapportering av avvik. Det er utarbeidet en avviksprosedyre for helsesystemene. Revisjonen har imidlertid ikke identifisert avviksrapporter. I kapittel 3.3.4 i *Styringssystemet for informasjonssikkerhet* er det spesifisert eksempler på avvik. Hva kommunen anser som avvik, er imidlertid ikke dokumentert som en del av styringssystemet. Dette medfører risiko for at avvik ikke rapporteres og behandles slik forskriften tilsier samt at svakheter/mangler i etablerte kontroller ikke blir forbedret.	Gul
5	§ 2-7 Organisering De etablerte ansvars- og myndighetsforhold for bruk og forvaltning av informasjonssystemet synes å være godt ivaretatt og dokumentert. Rådmann har delegert systemeierrollen til RO-lederne. IKT-avdelingen drifter systemene og er leverandør av IKT-tjenester i kommunen. RO-ledere har delegert utøvelse av systemeierrollen til systemansvarlig. Leder for Personal/organisasjon fungerer som sikkerhetsleder. Revisjonen savner imidlertid klare forventinger til ansvar og myndighet som ligger i rollene IKT-sikkerhetsleder og systemeier.	Gul
6	§ 2-8 Personell - Kompetanse og autorisasjon Alle systemer har innført tilgangskontroller. Tilganger styres etter hvilken rolle brukeren har i systemene og gis etter "Need to Now"-prinsippet. Det er den respektive RO ved tilsetningsansvarlig som bestiller autorisasjoner. Autorisering av brukere blir initiert av tilsetningsansvarlig. De sørger også for at taushetserklæring blir akseptert og underskrevet. Behovet for opplæring blir initiert av tilsetningsansvarlig.	Grønn
7	§ 2-9 Taushetsplikt Autorisering av brukere blir initiert av tilsetningsansvarlig. Vedkommende sørger også for at taushetserklæring blir akseptert og underskrevet.	Grønn
8	§ 2-10 Fysisk Sikring Alle servere, datalagringssystemer og datanettverkelektronikk er fysisk sikret. I tillegg til at datautstyr er plassert flere steder i kommunen, har også kommunen data lagret i lokaler som ligger utenfor deres kontroll gjennom Follo-IKT samarbeidet. Samarbeidet med Follo-IKT styres gjennom en databehandleravtale.	Grønn

Pkt	Fakta og vurderinger	Kvalitet
9	§ 2-11 – Konfidensialitet Alle systemer har tilgangskontroll. IT-avdelingen definerer brukere i systemene, mens RO-ene og systemeier tildeler rettigheter i fagsystemene. Avslutning av arbeidsforhold eller endringer skal meldes. Oppfølging av tildelte autorisasjoner, spesielt i applikasjoner, gjøres i liten grad. Mangelfullt vedlikehold og gjennomgang av tildelte autorisasjoner medfører risiko for at tildelte autorisasjoner ikke er i samsvar med brukers stilling, som for eksempel avdekke at behov for innsyn i personopplysninger ikke lenger er tilstedet.	Gul
10	§ 2-12 Sikring av tilgjengelighet RO-ene har i sine SLA-avtalene med IKT-avdelingen avtalt krav til tilgjengelighet. Disse avtalene setter føringer for dimensjonering og konfigurasjon av IT-systemene for å sikre tilgjengelighet. Backup tas av alle systemer. Katastrofelokasjon er avklart, der IT-systemer kan etableres dersom rådhuset skulle bli berørt. Daglige sikkerhetskopier lagres fysisk på rådhuset, mens månedlige arkiveres ved annen lokasjon. Revisjonen etterlyser bruk av risikovurderinger for identifisering av tiltak. Dette introduserer risiko for at ikke alle elementer til de prioriterte tjenestene kan rekonstrueres.	Gul
11	§ 2-13 Sikring av integritet Det er innført tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig.	Grønn
12	§ 2-14 Sikkerhetstiltak Det er etablert sikkerhetstiltak som skjermer systemene og hindrer forsøk på uautorisert bruk. Informasjonssystemene er organisert i ulike sikkerhetssoner og sikkerhetsbarrierer i henhold til veiledning fra datatilsynet. Overvåking av forsøk på uautorisert bruk gjøres imidlertid i liten grad.	Grønn
13	§ 2-15 Sikkerhet hos andre virksomheter Kommunen har opprettet databehandleravtaler med parter som behandler personopplysninger. Avtalene forplikter samarbeidspartner å tilfredsstille kravene i personopplysningsforskriften.	Grønn
14	§ 2-16 Dokumentasjon og lagring av rutiner og logger med hensyn til bruk av informasjonssystemene Dokumentasjon med betydning for informasjonssikkerheten arkiveres elektronisk, men hverken rutinebeskrivelser eller hendelseslogger, arkiveres systematisk i henhold til kravene i forskriften.	Gul

Pkt	Fakta og vurderinger	Kvalitet
15	§ 3 – Systematiske tiltak for behandling av personopplysninger Det gjøres få risikovurderinger i RO-ene. Dette medfører risiko for at internkontrollen i kommunen på IKT-siden blir ad-hoc basert og lite dokumentert. Forvaltningen mangler en helhetlig risikobasert tilnærning for styring og kontroll med IKT systemene. Dette medfører risiko for at kommunen ikke i tilstrekkelig grad sikrer at personopplysninger behandles systematisk og etter planlagte tiltak.	Gul

5.2. Vår konklusjon – Etterlevelse av sikkerhetsbestemmelsene i forskrften

Konklusjon: Tilfredsstiller Vestby kommune sikkerhetsbestemmelsene i personopplysningsforskriften?
Forskriften pålegger databehandler en risikobasert tilnærning i sitt arbeid med informasjonssikkerhet. IKT-avdelingen utfører risikovurderinger av sine tjenester og kommuniserer til kommunens ledelse behov for investeringer i tekniske sikkerhetstiltak. Kommunen mangler imidlertid klare retningslinjer for klassifisering av IT-systemer. Slik klassifisering er avgjørende for å kunne sikre en helhetlig vurdering og prioritering av risikoreduserende tiltak og målrettede investeringer. Dette medfører risiko for at sikkerhetsarbeidet blir ad-hoc preget og ikke helhetlig risikotilnærming som er i harmoni med kommunens sikkerhetsmål og risikoappetitt.

6. Problemstilling #3 – Overordnede mål, retningslinjer og rutiner for IT

6.1. Gjennomgang av problemstilling

For å sikre økt viksomhetsfokus i IKT-virksomheten bør kommunens ledelse etablere tilstrekkelig styring og kontroll med IKT. Dette vil bedre samhandlingen mellom IKT og kommunens tjenester ved at ledelsen får en klarere forståelse for IT-virksomhetens bidrag til dem.

Styring og kontroll bør baseres på kjente rammeverk. Et rammeverk bidrar også til å møte myndighetenes krav til IT-kontroller gitt i lover, forskrifter og annet regelverk, herunder Personopplysningsloven med forskrifter.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling basert på beste praksis – COBIT:

Pkt	Fakta og vurderinger	Kvalitet
	Problemstilling #3: **Er det etablert overordnede mål, retningslinjer og rutiner for IT i Vestby kommune?**	
1	<u>Strategisk planlegging</u> Det er etablert prosesser og/eller samhandlingsarenaer for gjensidig involvering i strategisk planlegging for å sikre at IT understøtter virksomhetens mål. *"IT-planen"* sammen med *"Personvern og informasjonssikkerhet for Vestby Kommune"* (styringssystemet for informasjonssikkerhet) er de styrende dokumentene for IKT i kommunen og har definert de overordende mål, retningslinjer og rutiner for IT. I tillegg til å være en plan for arbeidet med IKT i kommunen, har IT-planen også funksjon som innspill til budsjettarbeidet. Dokumentet *Personvern og informasjonssikkerhet for Vestby Kommune* omhandler ansvaret og hvordan arbeid med personvern og informasjonssikkerhet er inndelt i styrende del, gjennomførende del og kontrollerende del og er bygget opp etter retningslinjer utgitt av Direktoratet for forvaltning og IKT (Difi) og Helsedirektoratet. Dokumentet er å betrakte som styringssystemet for informasjonssikkerhet, og omfatter helseopplysninger som behandles i Gerica, Winmed og SOSIO. Sammen danner disse de styrende dokumentene for IKT i kommunen.	Grønn

Pkt	Fakta og vurderinger	Kvalitet
2	<u>Strategisk plan</u> Det er utarbeidet en strategisk plan – *IT-plan*, som viser hvordan IT-målene understøtter kommunens målsettinger. Denne inneholder relevante kostnadselementer, investeringer, regulatoriske krav. Planen mangler imidlertid: - Knytning mot kommunens målsettinger - Akseptabel risiko - Prioritering av IT prosjekter - Tydelige beskrivelser av roller og ansvar for informasjonssikkerhet IT-planen er ikke oppdatert siste år, og revisjonen har heller ikke identifisert resultater fra den kontrollerende delen av styringssystemet for informasjonssikkerhet. Revisjonen har heller ikke identifisert en oversikt over de prosjekter som ble besluttet, hvilke som ble påbegynt eller hvilke som er ferdigstilt.	Gul
3	<u>Operasjonelle IT-planer</u> De operasjonelle IT-planene som understøtter de strategiske planene er spesifisert i IT-planen.	Grønn
4	<u>Oppfølging, prioritering og styring av sentrale IT-prosjekter</u> Det er etablert prosesser mellom IKT og RO-ene for løpende oppfølging, forslag til prioritering samt styring av sentrale IKT-prosjekter. RO-lederne er premissgivere for overordende mål og strategier for IKT. Styring med IKT er delt inn i 4 IKT råd; Hjemmetjenesten/rehab/Sykehjem, Teknisk etat/PBG/Eiendom, Skole/barnehage/kultur og sentraladministrasjonen. De enkelte IKT-råd er bl.a. ansvarlig for: - Å sette mål for systemstøtten i sine arbeidsprosesser. - Sikre at tilstrekkelig utredning blir gjennomført før endringer i systemstøtten foreslås. - Sikre at tilstrekkelig planlegging blir gjort før oppstart av et IKT-prosjekt. - At endringsaktiviteter gjennomføres med tilstrekkelig kvalitet og kostnadseffektivitet. Personal og organisasjonssjef koordinerer samarbeidet mellom RO-ledere og IKT-rådene. I tillegg til å inneha rollen som sikkerhetsansvarlig, er han eier av IT-planen og står for budsjettinnspill via *IT-Plan for Vestby Kommune*. Alle prioriteringer gjøres og vedtas i ledergruppen sammen med rådmannen. Det finnes i tillegg en felles interkommunal IKT-tjeneste – IKT Follo. I tillegg til å ha et innkjøpssamarbeid, leverer IKT-Follo datatjenester for arkivsystemer, GEO-datasystemer og Økonomi.	Grønn

Pkt	Fakta og vurderinger	Kvalitet
5	Kvalitetsstyring Kommunen legger opp til en standardisert og hensiktsmessig tilnærming til kvalitetsstyring som understøtter kommunens krav og behov. Kommunen har imidlertid få kvalitetsmål knyttet til IKT, men IKT har etablert tjenesteavtaler med RO-ene som definerer tjenestekvalitet. Disse danner også grunnlaget for anskaffelser av teknologi og maskinvare-kapasitet. Rapportene danner også grunnlag for forbedringer av tjenesten, herunder tjenestekvalitet, roller og ansvar, håndtering av endringer samt prioritering av prosjekter.	Grønn
6	Etterlevelse av kvalitetssystemet Prosedyrer og rutiner for sentrale IT-prosesser som bidrar til å etterleve kvalitetssystemet er lite dokumentert. Det er små forhold, og rutiner gjøres av få personer. Dette medfører risiko for at: - Driftsoppgaver ikke gjøres enhetlig - Rutiner ikke gjøres til avtalt tid - Driftsrutiner blir personavhengig (nøkkelpersoner)	Gul

6.2. Vår konklusjon - Overordnede mål, retningslinjer og rutiner for IT

Konklusjon: Er det etablert overordnede mål, retningslinjer og rutiner for IT i Vestby kommune?

Kommunen har definert mål, strategier og retningslinjer for IKT i kommunen. Planen mangler imidlertid kriterier for klassifisering av informasjon og systemer. Akseptabel risiko omhandler kun helsesystemer. De styrende dokumentene benytter ulike beskrivelser av roller og ansvar for organisering av informasjonssikkerhetsarbeidet. Prioritering av IT prosjekter kommer ikke frem av IT-planen.

Dette kan medføre at informasjonssikkerheten ikke blir tilstrekkelig ivaretatt ved at:

- IT-systemer hverken forvaltes eller opererer innenfor akseptabel risiko
- Kritiske IT-prosjekter får ikke riktig prioritet
- Beskrivelser av roller og ansvar gir høy grad av tolking og preges av personlige preferanser
- Uklart ansvar for oppfølging av kommunenes etterlevelse av lover og forskrifter

7. Problemstilling #4 – Vestby Kommunes etterlevelse av god IT-skikk

7.1. Gjennomgang av problemstilling

Med god it-skikk menes de tiltak en virksomhet bør iverksette i forbindelse med sin bruk av IT for å imøtekomme kravene i det rettslige begrepet "betryggende kontroll", samt de krav som stilles i lover og forskrifter og allment aksepterte standarder. God it-skikk vil således være et dynamisk begrep.

ISACA Norge har utgitt rettledning for god IT-skikk. Dette omhandler:

Område	Beskrivelse
Overordnet styring og kontroll	Det bør innføres et rammeverk for styring av IKT. Dette vil bedre samhandlingen mellom IKT og forretningen ved: - økt forretningsfokus i IT-virksomheten - at ledelsen får en klarere forståelse for IT-virksomhetens bidrag til forretningen Denne type rammeverk bidrar også til å møte myndighetenes krav til IT-kontroller gitt i lover, forskrifter og annet regelverk, herunder Personopplysningsloven med forskrifter.
Dokumentasjon	Det bør foreligge dokumentasjon som viser samtlige IT-systemer og sammenhengen mellom disse. En samlet dokumentasjon bør bestå av: - Systemdokumentasjon - Brukerdokumentasjon - Driftsdokumentasjon. Dokumentasjonen bør omfatte automatiske og manuelle rutiner ifm IT-systemet.
Tilgangskontroll	Det er styret(privat virksomhet) og den daglige ledelsen som har ansvaret for at et tilfredsstillende nivå av tilgangskontroll innføres og opprettholdes. Ansvar for å ivareta sikkerhet er regulert i lov. Dersom deler av virksomhetens IT-behandling utføres av eksterne leverandører, fritar ikke dette ledelsen for kontrollansvaret. Med tilgangskontroll menes metoder for å tildele, endre, slette og føre kontroll med autorisasjon for tilgang til IT-ressursene for å opprettholde konfidensialitet, integritet og tilgjengelighet til informasjon. Personopplysningsloven gir bl.a. føring for tilgangskontroll. Informasjonssikkerhetsleder bør vedlikeholde den delen av virksomhetens sikkerhetspolicy som gjelder informasjonssikkerhet, gjøre den kjent i organisasjonen samt å se til at virksomhetens retningslinjer for informasjonssikkerhet blir fulgt. Inkludert i dette er retningslinjene for tilgangskontroll.

Område	Beskrivelse
Kontinuitet	Med kontinuitet menes her de tiltak en virksomhet iverksetter for å sikre avbrudd i den operasjonelle drift av sentrale og desentrale IT-systemer og derved oppnå et akseptabelt nivå av stabilitet. Tiltakene tar sikte på å redusere sannsynlighet for og konsekvensen av uønskede hendelser. For avbruddssituasjoner bør det foreligge dokumentert og innøvde handlingsplaner som begrenser konsekvensene for virksomheten og normalisere situasjonen innen en akseptabel tid og kostnader. Tilgjengelige sikkerhetskopier bør opprettes og arkiveres i lys av: - Akseptabel avbrudd for etablering av ulike tjenester ved alternativ lokasjon - Akseptabel tap av informasjon - Re-etablering av tjenester
Endringshåndtering	Som en følge av at IT-systemer er blitt mer kritiske og er av vital betydning for kommunen, bør endringer gjennomføres på en effektiv og kontrollert måte, til rett tid og med forventet resultat. Det bør derfor etableres retningslinjer, prosedyrer og instrukser for hvordan endringsarbeidet bør gjennomføres, herunder: - Endringsorganisasjon - Roller og ansvar - Arbeidsdeling - Kategorisering - Risikovurdering - Testing - Varsling
Bruk av internett.	Tilknytning til internett endrer trusselbildet radikalt. Det er derfor viktig at beslutningen om å koble sammen lokalnett med internett tas på bakgrunn av en totalvurdering av kommunes behov. Det bør etableres skriftlige retningslinjer samt prosedyrer og instrukser for administrasjon og oppfølging av nettforbindelsen, herunder: - Roller og ansvar - Risikovurdering - Tekniske forhold - Tekniske tiltak - Brukeres ansvar - Hjemmekontor

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling:

Pkt	Fakta og vurderinger	Kvalitet
	Problemstilling #4: **Følger Vestby Kommune god IT-skikk?**	
1	<u>Overordnet styring for IKT</u> Sikkerhetsmål og strategier er definert både i *IT-plan* og *Personvern for informasjonssikkerhet for Vestby Kommune*. I kommunen så er det RO-ledere sammen med rådmannen som danner styringsgruppen. Og det er styringsgruppen som setter mål for kommunens bruk av IT. Regler og rutiner for behandling av helseopplysninger i kommunen er basert på retningslinjer utgitt av Direktoratet for forvaltning og IKT (Difi) og Helsedirektoratet – som begge baserer seg bl.a.på kjente rammeverk - ISO27000 og CoBIT. Drift og forvaltning av de øvrige systemene er ikke basert på kjente rammeverk, men kommunen har pågående aktiviteter for å adoptere dette rammeverket til å også omfatte de øvrige IT-systemene i kommunen. De styrende dokumentene IT-planen og Personvern for informasjonssikkerhet for Vestby kommune, inneholder begge føringer for kommunenes: - sikkerhetsmål og strategier - retningslinjer - systemeiere - tilgangskontroller - endringshåndtering - skadelig programvare - overvåkning - kontinuitet og katastrofehåndtering Det er gitt retningslinjer og prinsipper for informasjonssikkerhet (hva som må gjøres for å etterleve strategien) i de styrende dokumentene. Men forutsetninger for å gjøre gode risikovurderinger – klassifisering og definering av hva som er akseptabel risiko, omhandler kun helsesystemene Gerica, Winmed og SOSIO. Risikovurderinger gjøres for andre systemer men dokumenteres i liten grad. Dette kan medføre at risikoer i kritiske systemer ikke blir identifisert og ivaretatt med nødvendige sikkerhetstiltak som sikrer at de forvaltes og opererer med akseptabel risiko i harmoni med kommunens mål og risikoprofil.	Gul
2	<u>Risikotilnærming</u> Det er gitt retningslinjer og prinsipper for informasjonssikkerhet (hva som må gjøres for å etterleve strategien) i de styrende dokumentene. Men forutsetninger for å gjøre gode risikovurderinger – klassifisering og definering av hva som er akseptabel risiko, omhandler kun helsesystemene Gerica, Winmed og SOSIO. Risikovurderinger gjøres for andre systemer men dokumenteres i liten grad. Dette medfører risiko for en helhetlig oppfølging av arbeidet med informasjonssikkerhet der behov for tiltak er i harmoni med kommunens mål og risikoprofil.	Gul

Pkt	Fakta og vurderinger	Kvalitet
3	Systemeiere Alle systemer har fått tildelt systemeiere, men beskrivelsen av rollen og tilhørende ansvar er ikke i harmoni mellom de styrende dokumentene – ref. punkt 1. Dette gjelder for eksempel oppgaver for oppfølging av tildelte autorisasjoner, verifikasjon av konfigurasjon for autorisasjon (oppbygging av tilgangsnivåer - roller), system og brukerdokumentasjon, brukeropplæring, endringskontroll. Dette gir rom for egne tolkninger preget av personlig preferanser.	Gul
4	Tilgangskontroll Tilgang til systemer krever godkjennelse. Alle brukere får tildelt en unik brukerid med tilhørende passord som er personlig for brukeren. For eksterne tilganger benyttes sterkere autentisering i tillegg til at data beskyttes mot innsyn. Det eksisterer mange brukerdatabaser. Rettigheter i systemene settes i de respektive systemer. Oppfølging av definerte brukere og tildelte autorisasjoner gjøres både av IKT og systemeier, men er lite strukturert (regelmessig og planlagt) og rapporteres/registreres ikke. I *IT-planen* synes ansvaret til systemeier for tilgangkontroll å være lite presist definert. Dette introduserer risiko for at utøvelse av rollen blir farget av personlige referanser og fokus.	Gul
5	Dokumentasjon av IT-systemer Kommunen har gitt retningslinjer for håndtering av system-, bruker- og driftsdokumentasjon der systemeier har ansvaret for system- og brukerdokumentasjon. IKT-avdelingen har ansvar for driftsdokumentasjon.	Grønn
6	Endringshåndtering Endringsordre, eller ønsker som ny funksjonalitet, kommer fra RO-ene (systemeiere) eller rådmann (pålegg fra staten) og tas opp i de ulike IT-rådene (4) – også for fremtidige behov. Det er IKT-rådene og styringsgruppen som tar avgjørelser om prioritering av prosjekter. Ved større endringer opprettes en prosjektgruppe. Denne gruppen godkjenner når endringene/oppgraderingen er klar til implementering. Prosjekt-gruppen består av personer med ulike funksjoner i tillegg til systemeier/ systemkoordinater. Endringer utføres og testes etter en fastsatt sjekkliste/arbeidsplan som dokumenteres i helpdesk-systemet. Det gjøres ingen klassifisering av endringer, men standardendringer, dvs. endringer som IKT kan gjøre uten å starte et prosjekt, er spesifiser i SLA-en som IKT har med RO-ene. Endringer relatert til rettelser i operativsystemer for servere og klienter samt programvare herunder Java, antivirus, office, adobe osv. gjøres ukentlig. Antivirus/malware signaturdatabaser oppdateres daglig. Det er innført automatiske systemer for håndtering av slike endringer (SCCM). Endringer som klassifiseres som kritiske, installeres fortløpende uten testing. Oppdateringer vurderes før installasjon og IT-avdelingen tester disse før utrulling.	Grønn

Pkt	Fakta og vurderinger	Kvalitet
7	Beskyttelse mot skadelig programvare Kommunen har innført teknologi som beskytter IT-systeme mot skadelig programvare. All internettrafikk blir også kontrollert i en proxyløsning. Nettverket er inndelt i ulike sikkerhetssoner. Det gjøres gjennomgang av regler i barrierer, men baseline (grunnkonfigurasjon) av regelsettet er ikke dokumentert. Dette gjør det vanskelig å avdekke eventuelle avvik i gjeldene regelsett.	Grønn
8	Overvåkes av IT-systemene Kommunen har etablert overvåkingssystemer for datalinjer, datanettverksutstyr, servere og e-posttjenester. Mekanismer som sikrer tilgjengelige ressurser for kritiske tjenester, er innført for IP-telefoni. Kvaliteten i tjenesten/leveransen på IKT, herunder henvendelser fra brukere, kapasitet samt tilgjengelighet linjer og tjenester, rapporteres til IKT-leder.	Grønn
9	Kontinuitet og katastrofeplaner Kommunen har sentralisert sine IT-tjenester. Dette gjør tilgangen til IT-systemer sårbar ved feil på datakommunikasjon. Videre vil feil på sentralt datautstyr berøre mange brukere. Kommunen har etablert kontinuitetsløsninger for enkelte tjenester, og noen lokasjoner har installert alternative kommunikasjonsløsninger. På datasentrene er tjenester implementert på tekniske plattformer som sørger for redundans i noe utstrekning. Det ble i 2009 igangsatt en prosess med sikte på å utrede kommunenes behov ved en eventuell katastrofe eller driftsstans. Sikkerhetskopier lagres i en brannsafe i samme lokaler som datasystemene. Sikkerhetskopier for siste måned lagres utenfor rådhuset. Revisjonen har ikke identifisert en helhetlig katastrofeplan som sikrer kommunenes tjenester og forpliktelser i en katastrofesituasjon og som omfatter IKT. IKT har etablert rutiner for etablering av enkelte kritiske systemer innenfor helse, personal og sak/arkiv. Til sammen gir dette en risiko for at kommunens evne til rekonstruering av informasjon og IT-systemer ikke er i samsvar med kommunenes forpliktelser.	Rød
10	Bruk av internett Kommunens datasystemer er beskyttet mot internett med brannmur. Det er innført teknologi som beskytter IT-systemene mot skadelig programvare. Sikker sone (helsenett) har i tillegg innført flere barrierer som skal sikre at helseopplysninger ikke kommer på avveie ved en brukerfeil eller kan komme på avveie innfor kommunen. Systemene er konfigurert slik at de ikke kan omgås av brukere. Kommunen tilbyr også tilganger til enkelte av sine systemer fra internett. Tjenesten sikrer sterk autentisering samt kryptering av all datatrafikk. Det gjøres gjennomgang av regler i barrierer, men baseline (grunnkonfigurasjon) av regelsettet er ikke dokumentert. Dette gjør det vanskelig å avdekke eventuelle avvik i gjeldene regelsett, og er i tillegg påkrevd i personopplysningsforskriftens § 2.14.	Gul

7.2. Vår konklusjon – Vestby Kommunes etterlevelse av god IT-skikk

Konklusjon: Følger Vestby Kommune god IT-skikk?

Vestby kommune følger flere av retningslinjene gitt for god IT-skikk.

Kommunen mangler imidlertid retningslinjer for klassifisering av verdier samt fastsettelse av akseptabel risiko. Slik klassifisering er avgjørende for tilstrekkelig å kunne sikre en helhetlig vurdering og prioritering av systemer og behov for etablering av risikoreduserende tiltak som igjen sikrer målrettede investeringer.

Ansvaret som ligger i rollen som systemeier er uklart presisert, og dette medfører at utøvelse av rollen ikke blir enhetlig, men preges av personlige preferanser.

Kontinuitetsplanene for IKT mangler knytning mot kommunens beredskapsplaner mtp å sikre prosesser som har størst prioritet. Dette kan medføre at kontinuitets- og katastrofeplaner for IT-systemene ikke understøtter kommunens kritiske prosesser.

8. Problemstilling #5 – Tilfredsstillende arbeidsdeling vedr. IT

8.1. Gjennomgang av problemstilling

Den overordnede ledelsen bør innføre en deling av roller og ansvar som utelukker muligheten for at en enkelt person skal kunne undergrave viktige prosesser. Ledelsen bør også sikre at de ansatte bare utfører de arbeidsoppgavene som er tillagt deres arbeidsområder og stillinger.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #5: **Er det tilfredsstillende arbeidsdeling vedrørende IT i Vestby kommune**		
1	IT-organisasjon Det er etablert en IT-organisasjon som understøtter RO-enes behov. Her vurderes behov jevnlig og krav til kompetanse tilpasses behovet og endringstakten til den enkelte RO.	Grønn
2	Roller og ansvar for IT-ansatte Det er etablert og kommunisert roller for ansatte i IT-avdelingen. IT-avdelingen består av fem personer hvor oppgavene innefor IKT er fordelt.	Grønn
3	Roller og ansvar som kvalitetsansvarlig (QA) innenfor IT IKT-fagansvarlig er gitt rollen og ansvaret som kvalitetsansvarlig (QA) innenfor IT. I regelmessige møter med IKT-leder rapporteres brukerhenvendelser, feilrettingssaker samt status på kvaliteten i IKT-tjenestene.	Grønn
4	Roller og ansvar innenfor risiko, sikkerhet og compliance IKT-leder er ansvarlig for informasjonssikkerheten i kommunen. Organisering av arbeidet er beskrevet i *IT-planen* og i *Styringssystemet for informasjonssikkerhet*. Systemeier er tildelt verdier (applikasjoner), da i hovedsak til RO-ledere. I sistnevnte er *Daglig ansvarlig* og *Systemansvarlig* gitt konkrete oppgaver ift tilgangskontroll og oppfølging av sikkerhetsarbeidet. I *IT-planen* synes ansvaret til systemeier å være lite presist og introduserer risiko for at utøvelsen av rollen kan bli farget av personlige preferanser og fokus.	Gul
5	Ansvar og roller innenfor eierskap til systemer og data Det overvåkes i liten grad at etablerte roller og fullmakter etterleves. I IT-planen synes ansvaret til systemeier for rapportering av sitt ansvar å være lite presist. Dette introduserer risiko for at forventet ansvar ikke blir ivaretatt i tilstrekkelig grad.	Gul

Pkt	Fakta og vurderinger	Kvalitet
6	Ansvarsdeling Ansvarsdeling (Segregation-of-Duties) i IT-virksomheten er implementert i den forstand at IT delegerer tilgang til systemet, mens den enkelte RO delegerer tilgang til sine systemer for å sikre at ikke enkeltpersoner alene kan kompromittere vesentlige prosesser, og at ansvaret er tilpasset arbeidsoppgavene.	Grønn
7	Avhengigheten til nøkkelpersoner Det er i noe utstrekning etablert rutiner som identifiserer og eventuelt reduserer avhengigheten til nøkkelpersoner, men pga størrelsen til IT-avdelingen vil det være vanskelig å unngå avhengigheten til dem.	Grønn

8.2. Vår konklusjon – Tilfredsstillende arbeidsdeling vedrørende IT

Konklusjon: Er det tilfredsstillende arbeidsdeling vedrørende IT i Vestby kommune?
Arbeidsdelingen vedrørende drift og forvaltning av IT i Vestby kommune, synes å være tilfredsstillende. Det er rom for nærmere avklaring og dokumentasjon av ansvaret som hviler på systemeier i lys av risiko, herunder etablering av tiltak samt å sikre etterlevelse av lover og forskrifter.

9. Problemstilling #6 – Rutiner for reetablering av IKT-tjenester etter driftsstans

9.1. Gjennomgang av problemstilling

Behovet for kontinuerlige IT-tjenester må ses i lys av kommunenes behov for kritiske og prioriterte tjenester. Dette krever utvikling, vedlikehold og testing av IT-kontinuitetsplaner/katastrofeplaner, tilgjengelighet til sikkerhetskopier og periodisk gjennomgang av katastrofeplanen. Formålet er å minimere utfallet av en eventuell hendelse med påfølgende avbrudd i IT-tjenestene.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling nedenfor samt i problemstilling #4, punkt 9:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #6: **Har Vestby kommune rutiner for å gjenoppta normal drift etter driftsstans?**		
1	<u>Rammeverk</u> Revisjonen har ikke identifisert at kontinuitets- og katastrofeplanene for IT-tjenester er basert på et rammeverk. IT har etablert noen manuelle rutiner for kritiske applikasjoner innen helse, personal sak og arkiv. Det er ikke kjent for revisjonen at kommunenes katastrofeplan omfatter IT-systemene utover telefonisystemene. Dette medfører en risiko for at kontinuitets- og katastrofeplanen ikke er dekkende for kommunens behov.	Gul
2	<u>Vedlikehold av kontinuitets- og katastrofeplaner</u> Revisjonen har ikke identifisert en prosess som sikrer regelmessig oppdatering av kontinuitets- og katastrofeplaner. IT-leder gjennomførte en utredning i 2009, men revisjonen har ikke identifisert noen beslutninger som følge av denne utredningen. IKT-avdelingen har allokert IKT-ressurser i lokasjoner utenfor rådhuset til benyttelse ved en katastrofe for reetablering av kritiske systemer innen helse, personal, sak og arkiv. Mangel på en helhetlig plan introduserer risiko for at kommunen ikke har tilstrekkelige planer for å sikre kommunenes tjenester og forpliktelser i en katastrofesituasjon.	Rød
3	<u>Testing</u> Test av reetablering av kritiske systemer innen helse, personell, sak og arkiv utføres av IT. Mangel på en helhetlig plan introduserer risiko for at kommunen ikke har tilstrekkelige planer for å sikre kommunenes tjenester og forpliktelser i en katastrofesituasjon - se problemstilling 4, punkt 9.	Gul

Pkt	Fakta og vurderinger	Kvalitet
4	Opplæring Det gjennomføres opplæring i de delene av kontinuitets- og katastrofeplanene som er utarbeidet. Mangel på en helhetlig plan introduserer risiko for at utførende personell ikke får tilstrekkelig opplæring og trening i etablering av kommunens tjenester og forpliktelser i en katastrofesituasjon.	Gul
5	Tilgjengelighet og distribusjon av planer Kontinuitets- og katastrofeplanene er ikke utarbeidet og er heller ikke distribuert til relevante personer. Mangel på en helhetlig plan introduserer risiko for at kommunens planer for å sikre kommunenes tjenester og forpliktelser i en katastrofesituasjon, ikke er kjent av de involverte.	Rød
6	Oppbevaring av backup Kritisk backup oppbevares utenfor hovedlokasjonen via et manuelt system på tape. Et automatisk backupsystem er under oppføring og vil være operasjonelt i løpet av desember måned. Dokumentasjon og planer oppbevares imidlertid ikke utenfor hovedlokasjonen. Mangel på en helhetlig plan introduserer risiko for at kommunen ikke har tilstrekkelige planer for å sikre kommunenes tjenester og forpliktelser i en katastrofesituasjon.	Gul
7	Evalueringer Det gjennomføres evalueringer etter hendelser hvor kontinuitets- eller katastrofeplaner for kritiske systemer innen helse, personell, sak og arkiv er vurdert. Revisjonen har ikke avdekket at andre områder er omhandlet i planer. Mangel på en helhetlig plan introduserer risiko for at kommunen ikke har tilstrekkelige planer for å sikre kommunenes tjenester og forpliktelser i en katastrofesituasjon.	Gul

9.2. Vår konklusjon – Rutiner for reetablering av IKT-tjenester etter driftsstans

Konklusjon: Har Vestby kommune rutiner for å gjenoppta normal drift etter driftsstans?
Det ble i 2009 igangsatt en utredning med sikte på å utrede kommunenes behov ved en eventuell katastrofe eller ved driftsstans. Det ble dog ikke utarbeidet helhetlige katastrofeplaner etter dette som berører IT. I de katastrofetestene som har blitt gjennomført så har IT kun vært involvert for å sikre telefoni. IT har selv utarbeidet planer for de mest kritiske systemene innen helse, personal og sak/arkiv. Det er imidlertid ikke utarbeidet en helhetlig dokumentert plan som er i samsvar med kommunes katastrofeplan.

10. Problemstilling #7 – Rutiner for endringshåndtering innen IT

10.1. Gjennomgang av problemstilling

For å redusere risikoen for uønskede hendelser som følge av endringer i programvare og infrastruktur, er det viktig at alle endringer, inkludert nødendringer og oppgraderinger, er formelt behandlet på en kontrollert måte. Endringer bør logges, vurderes og autoriseres før implementering og deretter evalueres for å se om endringen medførte den ønskede effekten.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling nedenfor samt i problemstilling #4, punkt 6:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #7: Har Vestby kommune rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?		
1	Prosess Det er etablert formelle endringsprosesser som omfatter alle typer endringer.	Grønn
2	Klassifisering Alle endringer vurderes, kategoriseres, prioriteres og godkjennes etter fastlagte kriterier.	Grønn
3	Nødendringer Det er etablert en formell prosess for håndtering av nødendringer.	Grønn
4	Oppfølging Alle endringer blir fulgt opp og status blir rapportert.	Grønn
5	Dokumentasjon Det er etablert rutiner for å sikre at system- og brukerdokumentasjon blir oppdatert når endringer implementeres.	Grønn

10.2. Vår konklusjon – Rutiner for endringshåndtering innen IT

Konklusjon: Har Vestby kommune rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?

Det er IKT-rådene og styringsgruppen som tar avgjørelsen om prioritering av prosjekter. Ved større endringer opprettes en prosjektgruppe. Endringer utføres og testes etter en fastsatt sjekkliste/arbeidsplan som dokumenteres i sakssystemet. Det gjøres ingen klassifisering av endringer, men standardendringer (dvs. endringer som IKT kan gjøre uten å starte et prosjekt) er spesifisert i SLA som IKT har med RO-ene.

Kommunen synes å ha etablert en prosess som sikrer tilfredsstillende kontroll med endringer i IT-systemene.

11. Problemstilling #8 – Overvåking av kritiske systemressurser

11.1. Gjennomgang av problemstilling

En viktig del av styringen av kommunens IT-ressurser er kontroll og overvåkning av maskinvare og linjer. Det er viktig å ha en prosess der en periodisk overvåker belastning på maskinvare, linjer, lagring og alternative backupløsninger. Denne prosessen er ment å gi en forsikring om at kommunen løpende klarer å levere de avtalte IT tjenestene til sine brukere.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling nedenfor samt i problemstilling #4, punkt 8:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #8: Er maskinkapasiteten god nok for å sikre stabil drift?		
1	Prosess Det er etablert en prosess for vurdering av ytelse og kapasitet i forhold til etablerte SLA-er og Vestby kommunes øvrige behov. IKT har regelmessige møter med RO-ene der krav til leveranse blir rapportert og gjennomgått.	Grønn
2	Overvåking Det er etablert et system for overvåkning av ytelse og kapasitet som følges opp av IKT.	Grønn
3	Fremtidig behov Det er etablert en prosess for vurdering av fremtidig behov for ytelse og kapasitet.	Grønn
4	Tilgjengelig kapasitet Det sikres at tilstrekkelig ytelse og kapasitet gjøres tilgjengelig. Telefoni er vurdert som mest kritisk og vil få høyest prioritet i datatrafikken.	Grønn
5	Rapportering Ytelse og kapasitet rapporteres jevnlig av IKT.	Grønn

11.2. Vår konklusjon – Overvåking av kritiske systemressurser

Konklusjon: Er maskinkapasiteten god nok for å sikre stabil drift?
Revisjonen har ikke funnet forhold som tilsier Vestby kommune ikke har rutiner for overvåkning og oppfølging av kritiske systemressurser.

12. Problemstilling #9 – Kompatibilitet mellom ulike datasystem

12.1. Gjennomgang av problemstilling

For å sikre konsistens i lagrede data bør det samme datagrunnlaget ligge til grunn i de ulike systemene. En slik modell bør beskrives og vedlikeholdes. Prosedyrer bør implementeres for å sikre integritet og konsistens i all lagret data.

Tabellen nedenfor viser funn og vurderinger fra vår gjennomgang av problemstilling:

Pkt	Fakta og vurderinger	Kvalitet
Problemstilling #9: Er kompatibiliteten mellom ulike datasystem i Vestby kommune tilfredsstillende?		
1	Vestby kommune har ikke etablert en informasjonsarkitektur/-modell som understøtter applikasjonsutvikling og annet informasjonsbehov som vedlikeholdes.	Rød
2	Det finnes ikke en data dictionary som beskriver hele virksomhetens lagrede data, og som sikrer deling av data mellom systemer og virksomhetsområder.	Rød
3	Få prosedyrer er implementert for å sikre integritet og konsistens i all lagret data i databaser, datavarehus og arkiv.	Gul

12.2. Vår konklusjon – Kompatibilitet mellom ulike datasystem

Konklusjon: Er kompatibiliteten mellom ulike datasystem i Vestby kommune tilfredsstillende?
Samme informasjon lagres i flere datasystemer. Dette fordrer manuelle handlinger for å sikre tilstrekkelig datakvalitet og er krevende. Mangel på prosedyrer for vedlikehold av denne informasjonen medfører risiko for at integritet og konsistens i lagrede data ikke blir tilstrekkelig ivaretatt.

13. Høringsuttalelse

Vestby kommune

13 desember 2012

BDO

Kommentarer til Rapport fra Forvaltningsrevisjon – Informasjonssikkerhet og IT-drift av 7/12

Rapporten peker på forhold som fungerer godt, tilfredsstillende og noen få forhold som må tas tak i for å tilfredsstille lover og forskrifter. Helsedelen av kommunen har som følge av at man har innført Normen som en sikkerhets- og prosedyre mal for Norsk Helsenett kommet lengst i forhold til å tilfredsstille samtlige lover og regler, med systematisk dokumentasjon av ROSanalysene er disse systemene i mål i forhold til å tilfredstille kravene. Resten av kommunen begynner i 2013 en prosess for å tilfredsstille kravene i "Plan for informasjonssikring i Vestby kommune " og vil når dette arbeidet er i mål ha slukket de røde og være godt i gang med å endre de gule lysene i rapporten til grønne.

Hovedfunn
Ut fra det vi kan forstå synes det som om dokumentasjon av risikoanalyser og enhetlig klassifisering av samtlige systemer, rolleplassering samt krise og katastrofeplaner dekker store deler av det som må tas tak i. Dette vil i alt vesentlig grad bli dekket av behandlingen av IKTplanen 2013 – 2016 og nevnte prosess som sluttføres i 2013.

Vedrørende rapportens oppbygging
Rapporten nevner mange av hovedfunnene under flere av hovedoverskriftene, noe som kan virke litt forvirrende i forhold til rapportens totale resultat. Enkelte av konklusjonene/rådene kan være vanskelig å forholde seg til da de ikke henviser direkte til funn i undersøkelsen, og blir derfor litt generelle i sin art.
Rapporten synes å være skrevet uten tilstrekklig hensyntagen til den struktur og det ledelseshierarki som er grunnlegende for drift og ledelse av kommunen. Det helhetlige ansvar som i de fleste hensenede pålegges ROledere og evt. videre nedover i organisasjonen gjennom delegasjonsreglementet synes ikke å være hensyntatt ift eksempelvis roller, ansvar og prioriteringer, noe som ikke skal hindre at dette blir klargjort ytterligere og dokumentert i gjennomgangen IKT/Systemeierne skal ha i 2013.
Enkelte av utsagnene om forhold som bør forbedres/endres blir ikke underbygget med eksempler på hva som bør forbedres/endres og kan derfor bli vanskelige å følge opp.

Rapporten formulerer seg noen ganger slik at det skapes tvil om det som kommenteres er reele funn. Dette kan skyldes at revisjonen ikke har hatt tilstrekkelig tid til å sette seg inn i alle kommunens prosesser og dens organisasjon. Det kan i ettertid være vanskelig å følge opp dette med tiltak. Eksempelvis;"Det er ikke kjent for revisjonen at kommunenes katastrofeplan omfatter IT-systemene utover telefonisystemene."

Svaret på dette er at kommunen blant annet har investert i generatoranlegg i rådhuset for å

hindre at IKTsystemene går ned i en av de mest relevante krises-senarioene for kommunen– strømbortfall.

Det pekes også på at IKTavdelingens katastrofeplan ikke er knyttet opp mot kommunens katastrofe og kriseplan – vi forstår da dette som beredskapsplanen. Det er i og for seg helt korrekt at det ikke foreligger beskrivelser av dette. I erkjennelsen av at en kommune er en stor og kompleks organisasjon som må ha beredskap for så å si alle mulige hendelser så er beredskapsplanen innrettet slik at det hos beredskapsledelsen til enhver tid skal forefinnes fagpersonell ift den relevante problemstillingen/krisen, med tilgang til sine relevante IKTsystemer. Vi har eksempelvis en geoingeniør i staben som sørger for tilgang til kart og geologidata. Rapporten peker imidlertid på noe vesentlig, og problemstillingen er etter vår mening løst gjennom måten man organiserer og bemanner beredskapsarbeidet på.
Kriseledelse er forøvrig sikret drift av samtlige lokale systemer selv om strømmen blir borte også om man må flytte til alternativ kommandoplass, da det er klargjort for strømaggeregat som kan holde kriseledelse med strøm for IKTdrift over lang tid.
Det er korrekt at IKTavdelingens egen katastrofeplan er for dårlig dokumentert. Den skal dokumenteres enda bedre og testes i året som kommer.

Vi vil kommentere noen av hovedfunnene ytterligere;

1.1 Oppsummering
Denne summerer korrekt nok opp det store bildet, men kunne gjerne konkretisert problemstillinger i forhold til de sentrale forhold som nevnes. De kommer imidlertid klarere frem senere i rapporten.
Av de mest omtale, gjentatte ganger repeterte problemstillingene introduseres mangelen på ”ferske” ROSanalyser og prioriteringer av ITsystemer i eventuelle kontinuitets- og katastrofeplaner. Vi ser behovet for å ta tak i en ROS gjennomgang, og har allerede kommentert katastrofeplaner, noe vi kommer ytterligere tilbake til.

1.2 Problemstilling 1
Her introduseres begrepet enhetlig klassifisering. Vi forholder oss til at denne klassifiseringen vil være resultatet av en ROSanalyse, og ser selvfølgelig nytten av en enhetlig begrepsverden/enhetlig perspektiv så langt det lar seg gjøre med rundt 100 større og mindre applikasjoner. Noe avhengig av viktigheten og kompleksiteten vil en helhetlig klassifisering bli foretatt. Gjennom forberedelsene til infrastrukturanskaffelsen 2011 – 2012 ble både kabling, nettverk og telefoni gjennomgått i forhold til risiko. Denne dokumentasjonen er dessverre ikke forelagt revisjonen, men vil bli nyttet i dokumentasjonsarbeidet.
Tilgangskontroll gjøres via systemeiers vurdering av behovet for brukernes rettigheter. Dette kan tas inn i systemeierrollebeskrivelsen i IKTplanen

1.3 Problemstilling 2
Ingen kommentarer utover det som allerede er sagt om ROS-analyser og klassifisering i problemstilling 1.

1.4 Problemstilling 3
Konsekvensene av at IT-prosjekter ikke kommer frem av IKTplanen synes for oss som er midt i situasjonen noe overdramatisert, da det ikke er mange store prosjekter og at

IKTavdelingen normalt er hovedutfører av samtlige prosjekter i samarbeid med gjeldende systemeier. Riktig store prosjekter er ofte en del av handlingsplanen og blir satt i sammenheng med de øvrige prosjektene i IKTavdelingens budsjett og handlingsplan. Prioriteringer av kjente prosjekter ved utarbeidelse av IKTplanen vil bli tatt inn. Ved endringer gjennom året vil planen bli revidert. Vi stiller oss imidlertid litt undrende til dimensjonen i slutningene i forhold til at det normalt forvaltes mellom 3 og 5 millioner pr år i investeringer.

1.5 Problemstilling 4

Alt tyder på at det som for den enkelte i ledelsen er en selvfølge i forhold til prioritet ved sikring, forebygging og evt. gjenoppretting ikke er godt nok dokumentert i planverket. Ved en rekovery situasjon havner alltid de ikke lovbestenmte systemene sist i prioritetskøen. Detaljeringgraden og fremdriften på en slik jobb vil være preget av ressurssituasjon i IKTavdelingen.

1.6 Problemstilling 5

Ingen kommentarer

1.7 Problemstilling 6

De katastroftetestene som omtales er det vi normalt kaller Beredskapsøvelser og det er i bestefall missvisende å si at det kun er telefoni som har vært IKTs bidrag. I kriseledelsen er det til enhver tid tilgang på saksbehandler verktøy/arkiv, internett, geografiske informasjonssystemer og de fagsystemene som er mest aktuelle. Ledelsenes tilgang til og bruk av ledelsesverktøy er alltid et viktig moment under våre beredskapsøvelser, forøvrig også et øvingsmoment vi har scoret høyt på. Se for øvrig under innledningen om samme tema.

1.8 Problemstilling 7

Ingen kommentarer

1.9 Problemstilling 8

Ingen kommentarer

1.10. Problemstilling 9

Det går ikke fram av rapporten hva slags informasjon/ hvilke systemer det siktes til som dobbeltlagres etc, og hva som fører til at det blir rødt lys. Funnet er korrekt og det vil fortsatt være slik at mye av informasjonen som legges i enkelte av systemene av sikkerhetsmessige grunner ikke skal kunne utveksles/deles/oppdateres sammen med andre systemer. For den informasjonen det er natulig å sambruke er dette pr dato ikke ett stort problem, men det arbeides mot en størst mulig integrering der tiltakene er tilrådelige, sikkerhetsmessig forsvarlig og kosteffektive.

1.10 Forslag til tiltak

1. Det er nødvendig å utarbeide en god katastrofeplan, men hva effekten av å harmonisere den med beredskapslanen er, er ukjent for oss, forholdet mellom disse planene er tidligere omtalt. I den grad recoveryrekkefølgen er forskjellig under normaldrift og ved eventuelle beredskaps/krisesituasjoner skal dette dokumenteres i IKTs driftsrutiner/IKTplanen så langt mulig.

2. Rådene tas ad notam
3. Systemeierne i Vestby kommune vil normalt ikke ha IKTkompetanse som dekker slike forhold, så i den grad de skal være ansvarlig for forhold som nærmer seg et teknisk nivå skal dette alltid gjøres i samarbeid med IKTavdelingen. Dette kan dokumenteres i IKTplanen under systemansvarligs ansvar.
5. Fokus på integrasjon er ett godt råd og til tross for mangel på ferske ROSanalyser er integrasjon og sambruk alltid i fokus ved anskaffelser. Funksjonalitet og brukervennlighet er også sentrale vurderingskriterier.

2.4 Avgrensninger og begrensninger
Dette er en fornuftig avgrensning.

3.Beskrivelse av IKT organisering, applikasjoner og roller i Vestby kommune
Synes å være en grei oppsummering ift hvordan det i praksis er.

4 – 12. En detaljert gjennomgang av problemområdene.

Grønt lys score
Det er gledelig å se at revisjonen finner at så å si alle tema som går på forvaltning og sikring av informasjon både lagret og mot evt. angrep utenfra har en grønt lys score, slik som; Samlet oversikt over verdier (prosesser, informasjon, ITsystemer), Sikkerhetsledelse, Personell - Kompetanse og autorisasjon, Taushetsplikt (oversikt), Fysisk sikring, sikring av integritet, sikkerhetstiltak for øvrig, Sikkerhet hos andre virksomheter (IKT Follo), Strategisk og operasjonell planlegging, oppfølging, prioritering og styring av sentrale IT-prosjekter, Kvalitetsstyring, dokumentasjon av IT-systemer, Endringshåndtering, Beskyttelse mot skadelig programvare (virus), Overvåkning av ITsystemene, IT organisasjon, roller og ansvar for ITansatte og QA innenfor IT, Ansvarsdeling og avhengighet av nøkkelpersoner (til tross for en liten bemanning), Rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon (problemstilling 7 i sin helhet), og God nok maskinkapasitet til å sikre stabil drift(problemstilling 8 i sin helhet). Disse områdene vil bli fulgt opp i forhold til IKTplanen og daglig forvaltning og utvikling.

Rødt Lys score
Problemstilling 9 (kompabilitet mellom ulike datasystemer.).
Det er ikke pekt på hvilke systemer det siktes til, det pekes imidlertid på at informasjon lagres i flere datasystem. Å tilpasse og vedlikeholde system og sikkerhetsprosedyrer slik at dette blir gjennomgående mulig er av oss beregnet til å bli mye mer ressurskrevende enn måten vi pr i dag behandler en del data på, i tillegg vil det ikke heve sikkerhetsnivået vesentlig, da de mest aktuelle systemene allerede har sterke sikkerhetsrutiner knyttet til databehandlingsrutinene - eks Gerica (Helsesystem), Esa, Agresso, Visma skole etc…. Vi har til tross for det som står beskrevet her flere system som deler informasjon. En begrenset koordinering, en enda bedre beskrevet informasjonsarkitektur, og en data dictionary vil bringe oss opp på ett godkjent nivå.

Kontinuitet og katastrofteplaner
Dette temaet tas opp i 2 – 3 av problemstillingene, spesielt nøye er det tatt opp under problemstilling 4, under henvisning til at det ikke er kobling mellom kommunens øvrige beredskaps/kriseplaner og slike planer for IKT. Vi har ikke vurdert dette som formålstjenlig

eller overkommelig rent ressursmessig. Kriseledelsen skal alltid etablere seg i lokaler som har nødstrømsanlegg som er dimensjonert for å drifte de nødvendige applikasjoner. Det er etablert redundans i store deler av kommunen (noe rapporten ikke synes å ha fått med seg i tilstrekklig grad), herunder til mulige alternative lokasjoner for kriseledelsen.
Det pekes på at å sentralisere ITtjenestene gjør oss mer sårbare. Det finnes sikkert mange teorier rundt dette, basert på forskjellige forutsetninger. I Vestby er IKTressursene så begrensede at samordning er alfa og omega for å sikre sambruk, effektiv drift og vedlikehold av både programvare og maskinvare. Drift og planlegging av IKTskole og resten av kommunen har tidligre vært drevet adskilt og erfaringene etter samordningen ift det å kunne planlegge helhetlig og allokere ressurser er utelukkende positive og fremmer kosteffektiv drift.

IKTavdelingens Kontinuitet og katastrofteutredninger og planer påbegynte arbeid fra 2009 er, som påpekt ikke sluttført, men vil få prioritet i 2013.

Det er også pekt på at det for flere av systemene, prosessene etc mangler oppdaterte Risikovurderinger/enhetlig klassifisering. Det stemmer og er ett utslag av knappe ressurser og stort arbeidspress, men vi ser at dette feltet må opprioriteres i tiden fremover, og det vil bli lagt en plan i prioritets rekkefølge for gjennomføring av risikovurderingene og enhetlig klassifisering for de enkelte system, prosesser og lokasjoner.

De gule trafikklysene
Det er forholdsvis mange gule trafikklys, og vi har bitt oss merke i at det er store ulikeheter ift dokumentasjonen i kommunen, i tillegg er det behov for å gå gjennom og presisere systemeier rollens ansvar og arbeidsoppgaver.
Begrepet (enhetlig) klassifisering blir også gulmerket under flere av problemstillingene. Vi har som skrevet antatt at klassifiseringen vil fremstå som godkjent og god nok etter en gjennomgang med risikoanalyser.
En annen måte å tilnærme seg begrepet klassifisering på er å tenke tilgangsskjerming. Kommunen har en oversikt over IT-systemene som inneholder personopplysninger. Hvert enkelt av disse systemene som behandler personellopplysninger, eksempelvis Helsesystemene, EsA(sak og arkiv), Agresso (Lønn, personal og regnskap), Skolesystemene, Barnehagesystemet etc har sine rutinebeskrivelser for dette. Kriteriene og regelsettene er dokumentert i hvert enkelt system. En samordning av dette ville være svært byråkratiserende og ikke gi merverdi.

Avslutning
Rådmannen finner ingen grunn til bekymring på grunnlag av denne rapporten, men har merket seg områder som må forbedres og områder som kan forbedres. Dette vil bli planlagt og gjennomført i sammenheng med utarbeidelsen av IKTplanen for 2013 – 2016, og innføringen av "Plan for informasjonssikring i Vestby kommune " i hele Vestby kommune i 2013. Det er ellers verdt å merke seg at en god del av manglene har oppstått grunnet kapasitetutfordringer, og alt tyder på at det ikke er mulig å gjennomføre disse forbedringene i forhold til formelle krav parallelt med ambisiøse IKTinvesteringer.

Rune Sletner
Personal og organisasjonssjef.