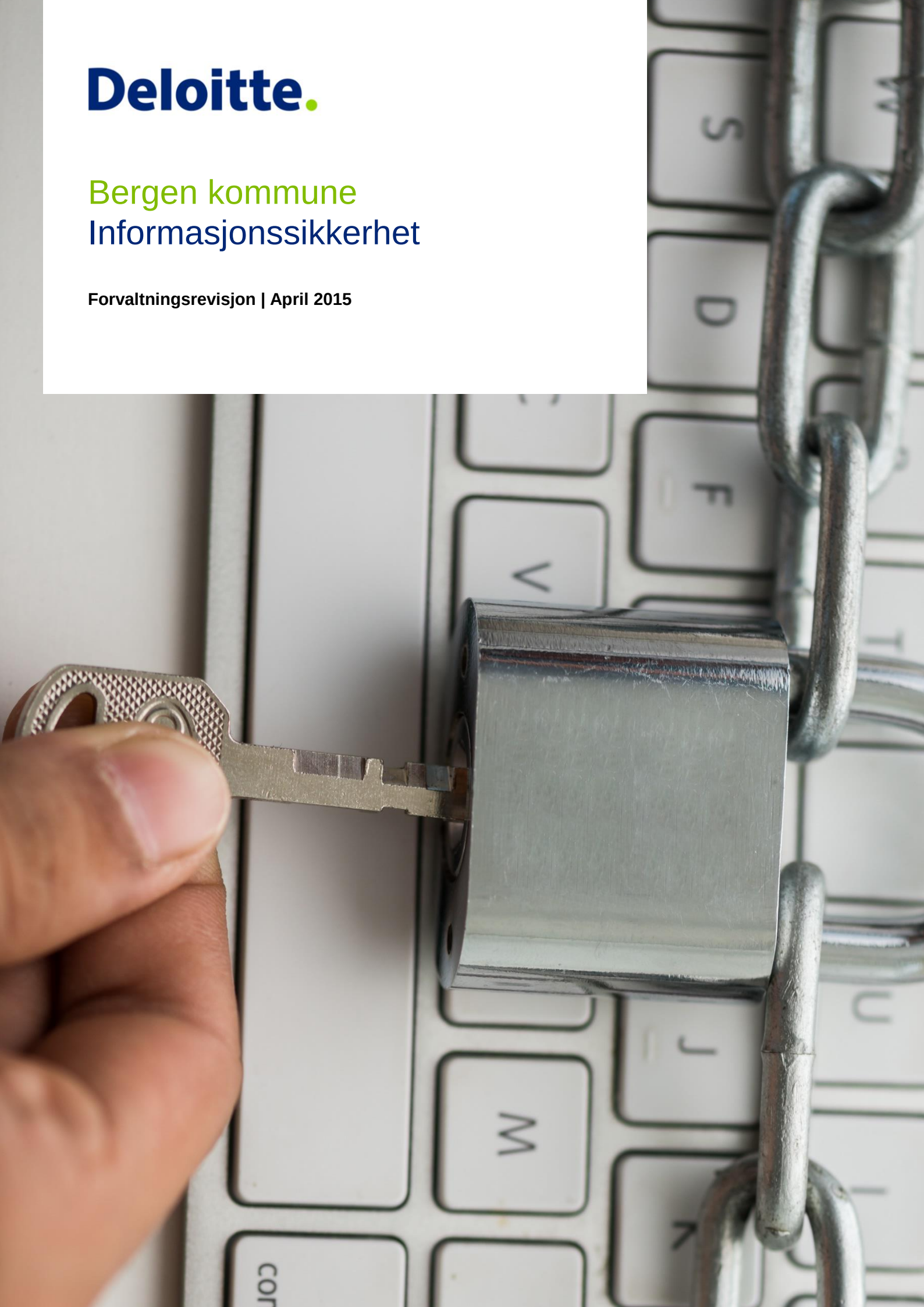
Deloitte.

Bergen kommune
Informasjonssikkerhet

Forvaltningsrevisjon | April 2015



Sammendrag

Deloitte har gjennomført en forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune. Forvaltningsrevisjonen er bestilt av kontrollutvalget i møte 8.4.2014. Formålet er å få kartlagt hvordan kommunen har fulgt opp funn og anbefalinger i oppfølging av forvaltningsrevisjonsrapporten «Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune», som ble utarbeidet i 2009.

Gjennomføring av forvaltningsrevisjonen

Revisjonen har gjennomgått rutiner og retningslinjer og gjennomført intervju med fem ledere og ansatte med spesielt ansvar knyttet til informasjonssikkerhet. I tillegg har det blitt gjennomført en spørreundersøkelse blant et utvalg ansatte i kommunen. Spørsmålene i undersøkelsen har vært basert på tilsvarende undersøkelse som ble gjennomført i forbindelse med forvaltningsrevisjonen i 2009.

Sammendrag av revisjonens vurderinger

Problemstilling 1: I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket knyttet til informasjonssikkerhet?

I forvaltningsrevisjonen i 2009 var en sentral anbefaling å etablere et informasjonssikkerhetssystem i samsvar med kravene i personopplysningsforskriften.

Revisjonens vurdering er at Bergen kommune siden den gang har satt i verk flere tiltak for å bedre informasjonssikkerheten og tilfredsstille krav i lovverket. Det er fastsatt en overordnet informasjonssikkerhetsstrategi for kommunen, og det er etablert en bedre oversikt over hvilke systemer og elektroniske tjenester som er i bruk i kommunen. I forbindelse med det strategiske informasjonssikkerhetsarbeidet og kartleggingen av systemer er det også gjennomført overordnede risikovurderinger knyttet til informasjonssikkerhet. Revisjonen vurderer at Bergen kommune har lagt til grunn et helhetlig perspektiv på informasjonssikkerhet gjennom å inkludere bl.a. samfunnssikkerhet og vern av materielle verdier, så vel som vern av elektronisk lagrede personopplysninger i arbeidet med informasjonssikkerhet. Videre er det gjennomført arbeid med databehandleravtaler med eksterne parter, samt utarbeidelse av rutiner og retningslinjer for informasjonssikkerhet for de delene av den kommunale virksomheten som er knyttet til Norsk helsenett.

Revisjonen mener samtidig at det på flere områder er mangler knyttet til styringssystemet for informasjonssikkerheten. Det går ikke klart fram av systemoversikten hvilke systemer som behandler personopplysninger, eller i hvilken grad disse er melde- eller konsesjonspliktige. Det er også etter revisjonens vurdering for lite tydelige retningslinjer for hvordan systemeiere skal gjennomføre risikovurderinger av sine systemer/tjenester. Videre er det ikke innført rutiner for sikkerhetsrevisjoner, og det er ikke skriftliggjort rutiner for «ledelsens gjennomgang» av informasjonssikkerhet. Det er innført en rutine for avviksregistrering, men spørreundersøkelsen viser at denne i liten grad er kjent blant de ansatte.

I den vedtatte strategien for informasjonssikkerhet er det flere tiltak som ikke har blitt gjennomført eller som har blitt vesentlig endret i den faktiske gjennomføringen. Revisjonen påpeker flere mulige årsaker til dette, bl.a. manglende ressurser, at tiltakene krever en høy prioritering av informasjonssikkerhet i hele organisasjonen, og at behov og kunnskap vil endres gjennom planperioden. Revisjonen mener

derfor at det ville være en fordel om strategien hadde stilt tydelige krav til frister, rapportering og eventuell rullering av tiltak.

Problemstilling 2: I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet tydeliggjort?

Revisjonen vurderer at det er områder hvor ansvar- og rollefordeling knyttet til informasjonssikkerhet kan tydeliggjøres i enda større grad enn i dag. På det overordnede, strategiske nivået er det i praksis noen av rollene som er beskrevet i informasjonssikkerhetsstrategien som ikke per i dag er virksomme. I dag brukes andre, eksisterende fora for å håndtere informasjonssikkerhetsspørsmål på dette nivået. Etter det revisjonen har fått opplyst vil ny informasjonssikkerhetsstrategi fastsette ansvars- og rollefordeling i samsvar med oppgave- og rollebeskrivelser som er under utarbeidelse i IKT Konsern.

Når det gjelder ansvar og oppgaver knyttet til informasjonssikkerhet på et «operasjonelt nivå», dvs. ute i organisasjonen, vurderer revisjonen at dagens oppgave og ansvarsfordeling ikke er tilstrekkelig tydelig. Systemeiere i organisasjonen er tillagt en rekke sentrale oppgaver i forbindelse med informasjonssikkerhet, men det går etter revisjonens vurdering ikke tilstrekkelig tydelig fram av retningslinjene hvordan de som har rollen som systemeier skal ivareta ansvaret.

Problemstilling 3: I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Revisjonen vurderer at Bergen kommune fremdeles har et klart forbedringspotensial når det gjelder de ansattes kjennskap til sentrale retningslinjer og instrukser knyttet til informasjonssikkerhet. Spørreundersøkelsen som er gjennomført blant de ansatte viser at det er mange av respondentene som ikke kjenner til sentrale retningslinjer, og det er mange respondenter som ikke kjenner til hvor man finner rutiner og retningslinjer for informasjonssikkerhet på Bergen kommunes intranett.

Videre er det også enkelte respondenter som påpeker at de savner «lokale» rutiner og retningslinjer og rutiner for hvordan man skal håndtere ulike typer personopplysninger, og det er flere som etterspør bedre opplæring knyttet til bl.a. oppbevaring av personopplysninger, taushetsplikt og sending og lagring av sensitiv informasjon. Basert på dette mener revisjonen at Bergen kommune bør iverksette effektive tiltak for å gi ansatte tilstrekkelig kunnskap om disse temaene.

Anbefalinger

IKT Konsern er nå i gang med et arbeid for å utbedre og konsolidere et styringssystem for informasjonssikkerhet. Dette arbeidet vil stå sentralt i det videre arbeidet med informasjonssikkerhet i kommunen. Med bakgrunn i funnene i denne forvaltningsrevisjonen anbefaler revisjonen at Bergen kommune vurderer å gjennomføre følgende tiltak:

1. Utbedre de elementene i styringssystemet hvor det er påpekt mangler, med særlig vekt på
   a) risikovurderinger
   b) sikkerhetsrevisjoner
   c) avvikshåndtering
   d) ledelsens gjennomgang
2. Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.
3. Sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert og sikre at alle ansatte kjenner til hvor man finner rutinene.
4. Ved utarbeidelse av ny strategi for informasjonssikkerhet, fastsette krav til oppfølging av og rapportering på gjennomføring av tiltak, samt eventuell rullering av planer og tiltak.

* * *

Byrådsavdeling for finans, eiendom og eierskap har gitt en uttale til rapporten og disse anbefalingene. Uttalen er lagt ved i rapportens vedlegg 2.

Innhold

1 Innledning

Deloitte har gjennomført forvaltningsrevisjon av informasjonssikkerhet og behandling av personopplysninger i Bergen kommune. Forvaltningsrevisjonen er bestilt av kontrollutvalget i møtet 8.4.2014 (sak 23-14).

1.1 Bakgrunn

I denne rapporten vurderer vi Bergen kommunes oppfølging av forvaltningsrevisjonsrapporten «Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune», som ble utarbeidet i 2009.

Rapporten fra 2009 hadde som formål å undersøke om Bergen kommune hadde tilfredsstillende system og rutiner for informasjonssikkerhet i forbindelse med behandling av personopplysninger, og om gjeldende regelverk ble fulgt. Datagrunnlaget var dokumentgjennomgang, intervjuer og spørreundersøkelse.

Forvaltningsrevisjonen konkluderte bl.a. med at Bergen kommune ikke oppfylte krav i personopplysningsforskriften på flere områder. Det ble pekt på mangler knyttet til bl.a.

- styringsdokumenter knyttet til informasjonssikkerhet
- oversikt over personopplysninger
- gjennomføring av sikkerhetsrevisjoner
- dokumentasjon av informasjonssikkerheten

Rapporten anbefalte å utbedre og oppdatere styrende dokumentasjon og rutiner, sikre at ansatte har nødvendig kunnskap om informasjonssikkerhet og tydeliggjøre ansvar og oppgaver knyttet til informasjonssikkerhet i kommunen. Rapporten ble behandlet i bystyret 25.1.2010.

1.2 Formål og problemstillinger

Formålet med prosjektet er å få kartlagt hvordan kommunen har fulgt opp funn og anbefalinger i forvaltningsrevisjonsrapporten.

Følgende problemstillinger er undersøkt i revisjonen:

1. I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket knyttet til informasjonssikkerhet?
   a) Er det innført rutiner og retningslinjer i samsvar med anbefalingene fra rapporten i 2009
   b) I hvilken grad er det gitt føringer for å sikre en helhetlig tilnærming til informasjonssikkerhet i kommunen?
2. I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet tydeliggjort?
3. I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

2 Metode

Forvaltningsrevisjonen er gjennomført i samsvar med kravene i RSK 001, standard for forvaltningsrevisjon.

2.1 Gjennomgang av dokumentasjon

Vi har gjennomgått rutinene for informasjonssikkerhet som IKT Konsern har gjort tilgjengelige på Bergen kommunes intranett. Vi har også gått gjennom arbeidsdokumenter som er i bruk i IKT Konsern, bl.a. oversikten over systemer og tjenester som er i bruk i kommunen. Fra IKT Drift har vi fått oversendt, og vi har gjennomgått, dokumentasjon knyttet til IKT Drifts eget styringssystem for informasjonssikkerhet, samt ekstern revisjonsrapport. Til sist har vi gått gjennom vedtak i bystyret og byrådet med relevans for området.

2.2 Intervju

I prosjektet er det gjennomført fem intervjuer:

- Leder for informasjonssikkerhet (IKT Konsern)
- Operativ leder for informasjonssikkerhet (IKT Drift)
- Direktør for IKT Konsern
- Kommunaldirektør for BFEE
- IKT-koordinator ved byrådsavdeling for helse og omsorg (BHO) og byrådsavdeling for sosial, bolig og områdesatsing (BSBO)

Alle som ble intervjuet fikk oversendt skriftlig referat av intervjuet og har verifisert referatet (dvs. godkjent og gjort eventuelle rettinger i referatet). Det er de verifiserte versjonene av intervjuene som blir brukt som datagrunnlag.

2.3 Spørreundersøkelse

Det er sendt ut en spørreundersøkelse til 692 ansatte i Bergen kommune. Utvalget av respondenter ble gjort som en tilfeldig trekking på bakgrunn av en oversikt over alle ansatte som er brukere av Bergen kommunes IT-systemer med egen e-postadresse.[1] Det var 337 respondenter som svarte på undersøkelsen.

Spørsmålene i undersøkelsen er basert på tilsvarende undersøkelse som ble sendt ut i forbindelse med forvaltningsrevisjonen som ble gjennomført i 2009.Der hvor vi har relevante tall å sammenligne med mellom 2009 og 2014, gjengir vi dette i rapporten. Det er likevel viktig å ta forbehold om at utvalgsmetoden brukt i de to undersøkelsene er ulik. I 2009 ble det gjennomført et begrenset utvalg basert på e-postlister fra ulike PPT-kontorer og skoler, mens data i 2014 ble valgt fra en oversikt over alle ansatte i Bergen kommune. For å gjøre sammenligningen enklere har vi, i tillegg til tall for alle respondenter i undersøkelsen, også brutt svarene fra 2014-undersøkelsen ned etter om de har sitt primære arbeidssted i PPT, skole eller andre enheter.

[1] Før den tilfeldige trekkingen ble enkelte grupper av ansatte fjernet fra listen. Dette gjelder: personer som arbeider i kommunalt AS, politikere, personer som har stillingsprosent under 40 %, ekstrahjelper, vikarer mv., samt enkelte stillingstyper (assistenter, renholdere, studenter, pensjonister).

2.4 Verifisering og høring

Alle intervjureferater er verifisert av intervjupersonene. Rapportens datadel er sendt til Bergen kommune for verifisering, og er justert på bakgrunn av tilbakemeldinger etter verifiseringen. Rapport med vurderingsdel er også sendt til Bergen kommune ved byrådsavdeling for finans, eiendom og eierskap til høring og uttale.

3 Revisjonskriterier

I dette kapittelet presenterer vi revisjonskriteriene for rapporten. Revisjonskriteriene er de kriteriene som praksis i kommunen vil vurderes opp mot. De er utledet i samsvar med krav i standard for forvaltningsrevisjon, RSK 001.

3.1 Regelverket om informasjonssikkerhet

Informasjonssikkerhet innebærer at personopplysninger og annen informasjon skal beskyttes mot uberettiget innsyn, og at den skal bli ivaretatt og være tilgjengelig for de som skal ha tilgang til den.

3.1.1 Personopplysningslov og –forskrift

Regelverket knyttet til informasjonssikkerhet omfatter bl.a. personopplysningslov og -forskrift. I personopplysningsforskriften er det gitt utfyllende bestemmelser og veiledninger knyttet til informasjonssikkerhet. «Sikkerhetsbestemmelsene» i forskriften (§ 2) pålegger virksomheter som behandler personopplysninger å

- fastsette sikkerhetsstrategi for virksomheten (§ 2-3)
- gjennomføre risikovurderinger etter fastsatte kriterier (§ 2-4)
- etablere klare ansvars og –myndighetsforhold for bruk av informasjonssystem (§ 2-7)
- etablere fysiske og tekniske tiltak for informasjonssikkerhet (§§ 2-10 til 2-14)
- sørge for at de ansatte har tilstrekkelig kunnskap om informasjonssikkerhet (§ 2-8)
- gjennomføre sikkerhetsrevisjoner for å etterprøve at tiltak er iverksatt og fungerer (§ 2-5)
- behandle uønskede hendelser i informasjonssystemet som avvik (§ 2-6)
- foreta regelmessig ledelsesgjennomgang av sikkerhetsmål og –strategi (§ 2-3)
- sikre at det ikke overleveres personopplysninger elektronisk til andre virksomheter dersom disse ikke tilfredsstiller kravene i sikkerhetsbestemmelsene (§ 2-15)

Den som primært har ansvar og plikter etter personopplysningsloven omtales i regelverket som «behandlingsansvarlig». Behandlingsansvarlig, representert ved den administrative ledelsen i virksomheten, bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.

3.1.2 Krav til styringssystem for informasjonssikkerhet

Et styringssystem for informasjonssikkerhet er et system som samler prosedyrer, rutiner og dokumentasjon knyttet til informasjonssikkerhet. Kommunen er gjennom bl.a. eForvaltningsforskriften § 15 forpliktet til å ha en internkontroll basert på anerkjente standarder for styringssystem for informasjonssikkerhet:

> *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. […]*

Med «anerkjent standard» for styringssystem menes en standard som ISO/IEC 27001.[2] Dette er en standardisering av styringssystem for informasjonssikkerhet som er utarbeidet av internasjonale organisasjoner.[3] Når man har innrettet styringssystemet etter denne standarden kan man en uavhengig akkreditert revisor sertifisere at virksomhetens styringssystem er i samsvar med kravene i standarden.

3.1.3 Annet regelverk

I tillegg til kravene i personopplysningsforskriften er det også flere andre regler knyttet til informasjonssikkerhet som er relevant i kommunen. Til dels er kravene i disse regelverkene overlappende med kravene til et styringssystem for informasjonssikkerhet.

I helseregisterloven er det gitt konkrete bestemmelser knyttet til håndtering av helseopplysninger, og her fremkommer det bl.a. konkrete krav knyttet til informasjonssikkerhet (§ 16). Det er utarbeidet en norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (*Normen*), som stiller krav med utgangspunkt i både personopplysningsforskriften og helseregisterloven. I normen er det også innarbeidet ulike krav knyttet til taushetsplikt og informasjonsrett etter særlovgiving for kommunehelsetjenester, sosialtjenester, psykisk helsevern, samt forvaltnings- og offentlighetslov.

Kommunen er også omfattet av sikkerhetsloven, og har som følge av dette plikt til å ha betryggende informasjonssikkerhet for informasjon som kan være kritisk for å forhindre trusler som spionasje, sabotasje og terrorhandlinger. Disse kravene kan være relevante for kommunen f.eks. når det gjelder å beskytte vannforsyningen fra forurensing av drikkevann.[4]

3.2 Kommunale vedtak knyttet til informasjonssikkerhet

3.2.1 Forvaltningsrevisjonsrapport om informasjonssikkerhet (2009)

Forvaltningsrevisjonsrapporten fra 2009 om informasjonssikkerhet konkluderte med at Bergen kommune bør:

- Opprettholde fokus på arbeidet med det nye systemet for informasjonssikkerhet,[5] og sikre at dette ivaretar kravene i personopplysningsforskriften, bl.a. når det gjelder
  - risikovurderinger
  - sikkerhetsrevisjon
  - avvikshåndtering
  - dokumentasjon
  - sikkerhet hos kommunikasjonspartnere og leverandører

- Sørge for at rutiner og retningslinjer knyttet til informasjonssikkerhet holdes oppdatert og blir tilstrekkelig implementert på alle nivå i kommunen, samt at medarbeiderne har nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner.

- Tilrettelegge for et godt samarbeid mellom de ulike aktørene som er involvert i kommunens IKT arbeid, og utarbeide skriftlige rollebeskrivelser som tydeliggjør ansvar og oppgaver.

3.2.2 Informasjonssikkerhetsstrategi for Bergen kommune (2011)

Bystyret vedtok i 2011 informasjonssikkerhetsstrategi for Bergen kommune. Strategien omfatter bl.a. to fokusområder for arbeidet med informasjonssikkerhet:

---

[2] Difi har fått i oppgave å gi anbefalinger på informasjonssikkerhetsområdet i tilknytning til denne paragrafen i eForvaltningsforskriften. I sin referansekatalog anbefaler Difi å basere seg på ISO/IEC 27001:2013 ved etablering av internkontroll/styringssystem på informasjonssikkerhetsområdet. I arbeidet med å implementere relevante tiltak (kontroller) anbefales det å følge strukturen i vedlegg A i ISO/IEC 27001:2013 og innholdsmessig støtte seg på ISO/IEC 27002:2013.

[3] International Organization for Standardization (ISO) og International Electrotechnical Commission (IEC).

[4] Jf. Drikkevannsforskriften § 14.

[5] Når rapporten fra 2009 beskriver «det nye systemet for informasjonssikkerhet» vises det til at kommunen på dette tidspunktet hadde satt i gang et arbeid med å systematisere styringsdokumentene knyttet til informasjonssikkerhet, og at retningslinjer og rutiner skulle samles på en egen intranettside.

- Organisering, systematikk og styring: *Bergen kommune skal iverksette systematiske tiltak for å tydeliggjøre, følge opp og dokumentere den enkeltes ansvar for informasjonsressurser og behandlingsprosesser*

- Informasjon, bevisstgjøring og sikkerhetskultur: *Bergen kommune skal iverksette tiltak for å tilby integrert opplæring og informasjon om informasjonssikkerhet som i størst mulig grad er tilpasset, tilgjengelig og teknologinøytral, samt tilstrebe at informasjonssikkerhet blir en naturlig del av kommunens organisasjonskultur*

4 Data

4.1 Organisering og styringssystem for informasjonssikkerhet

Vi vil under presentere gjeldende strategi, organisering, rutiner og prosedyrer for informasjonssikkerhet.

I intervju blir det forklart at Bergen kommune ennå ikke har et fullverdig styringssystem for informasjonssikkerhet, og at det er mangler i «overbygget» for rutinene på informasjonssikkerhetsområdet. Direktør for IKT Konsern peker i intervju på at man i dag nærmer seg et fullstendig styringssystem for informasjonssikkerhet. Selv om det mangler en del på formaliseringen av dette systemet, er de fleste av komponentene som et slikt system består av på plass. Det går videre fram av intervju at kommunen er i gang med et arbeid med å samle rutinene i et felles styringssystem (se 4.1.7).

4.1.1 Strategi for informasjonssikkerhet

Strategi for informasjonssikkerhet i Bergen kommune fra 2011 (se 3.2.2, over), som gjelder for perioden 2011 til 2014, gir noen generelle føringer for informasjonssikkerhet. Det går fram av strategien at Bergen kommune har en visjon om «en organisasjon med fokus på informasjonssikkerhet i alle ledd, hvor informasjonssikkerhet håndteres planmessig og systematisk og blir en naturlig del av organisasjonskulturen.» Det påpekes at økt bruk av IKT fører til større utfordringer for informasjonssikkerheten ved at informasjon behandles og blir spredt i større grad enn tidligere. Videre påpekes det at informasjonssikkerhet omhandler mer enn teknologi, og det vektlegges at det er viktig at alle medarbeidere kjenner sitt eget og andres ansvar for å bidra til økt informasjonssikkerhet. Det vises til tidligere arbeid med informasjonssikkerhet, samt til nasjonale føringer og krav i regelverk knyttet til informasjonssikkerhet. Det blir særlig lagt vekt på kravene til informasjonssikkerhet i personopplysningsforskriftens kapittel 2.

Informasjonssikkerhetsstrategien presenterer to fokusområder for arbeidet med informasjonssikkerhet *organisering, systematikk og styring* og *informasjon, bevisstgjøring og sikkerhetskultur*. I tilknytning til førstnevnte fokusområde går det fram at Bergen kommune skal «iverksette systematiske tiltak for å tydeliggjøre, følge opp og dokumentere den enkeltes ansvar for informasjonsressurser og behandlingsprosesser». I tilknytning til det andre fokusområdet går det fram at «Bergen kommune skal iverksette tiltak for å tilby integrert opplæring og informasjon om informasjonssikkerhet som i størst mulig grad er tilpasset, tilgjengelig og teknologinøytral, samt tilstrebe at informasjonssikkerhet blir en naturlig del av kommunens organisasjonskultur».

Innenfor fokusområdet organisering, systematikk og styring er det satt følgende «strategiske tiltak»:

1. Konkret tiltaksplan innen styringssystemets enkelte segmenter utarbeides og revideres årlig.
2. Revidere eksisterende instrukser og retningslinjer, og etablere nye ved behov.
3. Etablere styringssystem for informasjonssikkerhet med utgangspunkt i "Norm for informasjonssikkerhet i helsesektoren".
4. Kartlegge og klassifisere alle vesentlige informasjonsbehandlinger med hensyn til sikkerhetskrav.
5. Gjennomføre overordnete risikovurderinger innen hver byrådsavdeling og andre naturlig avgrensete organisatoriske enheter.
6. Foreta jevnlige sikkerhetsrevisjoner.
7. Etablere elektronisk støttesystem for å ivareta styrings- og internkontrollsystem for informasjonssikkerhet og andre områder med tilsvarende behov, som HMS-arbeidet.
8. Styrke bemanningen innen informasjonssikkerhet.

Innenfor fokusområdet informasjon, bevisstgjøring og sikkerhetskultur er det satt følgende tiltak:

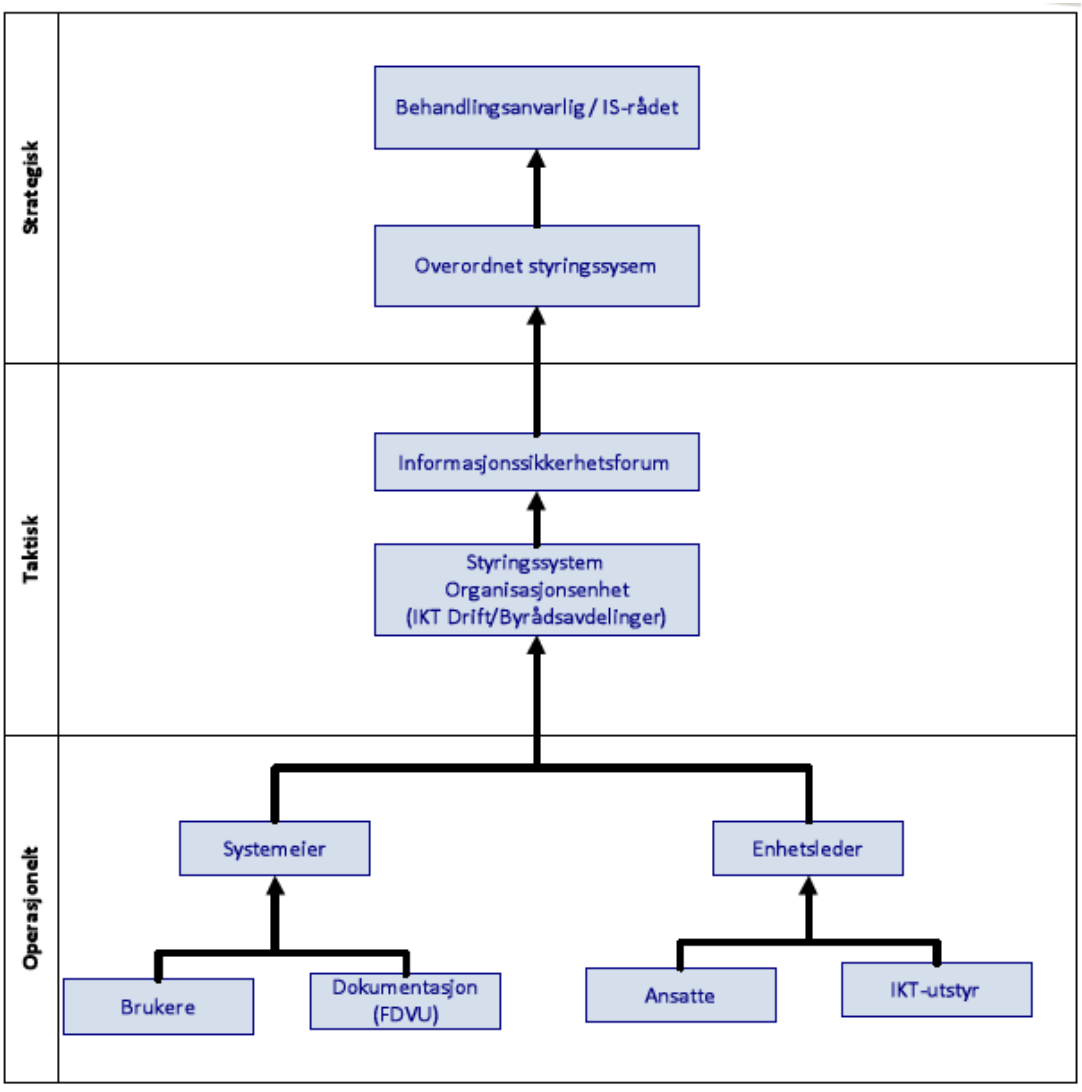
1. Integrere grunnleggende instrukser for sluttbrukere i personal- og arbeidsreglementet.
2. Standardisere krav til kartlegging, klassifisering, risikovurdering og avvikshåndtering.
3. Erstatte dagens løsning med automatisk fornying av IT-sikkerhetserklæringen en gang i året, med en grunnleggende e-læring for informasjonssikkerhet knyttet til personal og arbeidsreglementet.
4. Etablere styringskort for informasjonssikkerhet blant ledere.
5. Integrere kursmoduler for informasjonssikkerhet i eksisterende HR-kurs.
6. Utarbeide og tilgjengeliggjøre en oversiktlig og informativ struktur for instrukser, retningslinjer og andre styrende dokumenter.
7. Jevnlig informere organisasjonen om utviklingen i trusselbildet.

Det framgår ikke nærmere fastsatte frister eller noen beskrivelse av hvordan man skal følge opp og rapportere om status på tiltakene.

4.1.2 Sikkerhetsledelse og organisering

Organiseringen av informasjonssikkerhetsområdet er beskrevet i strategien. Her går det fram at informasjonssikkerhet er delt i tre nivåer: strategisk, taktisk og operasjonelt (jf. figur 1 under).

Figur 1 Organisasjonskart for arbeidet med informasjonssikkerhet (fra informasjonssikkerhetsstrategien)



Det går fram av strategien at byrådsleder er øverste behandlingsansvarlig, og derfor ansvarlig for all informasjonsbehandling som foregår i virksomheten. Behandlingsansvaret er videre delegert til kommunaldirektør for hver byrådsavdeling. Behandlingsansvarlige er på det strategiske nivået, hvor de overordnete føringene og styrende dokumentene besluttes. Strategien slår fast at byrådsleder er øverste behandlingsansvarlig, og at behandlingsansvaret er delegert til kommunaldirektør i de enkelte byrådsavdelingene (og direktør for bystyrets kontor). I tillegg til behandlingsansvarlige plasserer også strategien informasjonssikkerhetsansvarlig (ISA) og informasjonssikkerhetsrådet (IS-rådet) på det strategiske nivået. I informasjonssikkerhetsstrategien omtales IS-rådet, bestående av strategisk styringsgruppe, andre behandlingsansvarlige og informasjonssikkerhetsansvarlig, som det øverste styrende organet for informasjonssikkerhet. Det går fram av intervju at IS-rådet ikke har hatt møter, og at man i stedet har brukt eksisterende fora i IKT-organiseringen, samt at informasjonssikkerhetsansvarlig (leder for informasjonssikkerhet) har hatt dialog med byrådsdirektørene.

Av informasjonssikkerhetsstrategien går det fram at de strategiske føringene skal omsettes i praksis på et taktisk nivå, og gjennomføres i samarbeid med operasjonelt nivå. På det operasjonelle nivået skal informasjonssikkerheten ivaretas innen det enkelte ansvarsområde i henhold til instrukser. Resultatenhetsledere, ansatte og system- og tjenesteeiere hører til dette nivået.

4.1.2.1 IKT Konsern og leder for informasjonssikkerhet

Informasjonssikkerhetsansvarlig har *det overordnete ansvaret for informasjonssikkerheten for konsernet Bergen kommune*. Rollen til informasjonssikkerhetsansvarlig er forklart på følgende måte:

> I Bergen kommune er det IKT-sikkerhetsansvarlig som har det overordnete ansvaret for informasjonssikkerheten for konsernet Bergen kommune. Ansvaret innebærer å organisere, koordinere og styre sikkerhetsarbeidet på vegne av de daglig behandlingsansvarlige. Dette innebærer blant annet å etablere og vedlikeholde et overordnet styringssystem for informasjonssikkerhet, iverksette egenkontroll, gjennomføre forbedringsprosesser samt følge opp at sikkerheten vedlikeholdes i alle ledd.
>
> ISA har videre myndighet og ansvar til blant annet å kunne gjennomføre opplæring i informasjonssikkerhet, overordnete risikovurderinger, bestille sikkerhetstester, avvikshåndtering, iverksette korrigerende og andre sikkerhetsrelaterte tiltak. ISA rapporterer til daglig behandlingsansvarlige både innenfor den enkelte byrådsavdeling og gjennom IS-rådet i sikkerhetssaker.

Leder for informasjonssikkerhet (tidligere informasjonssikkerhetsansvarlig) forklarer i intervju at hans rolle i utgangspunktet handler om å drive med strategisk informasjonssikkerhetsarbeid. Dette innebærer bl.a. å få temaet inn på kommunaldirektørenes agenda. Leder for informasjonssikkerhet gir uttrykk for at han nå har mer direkte kontakt med kommunaldirektørene, sammenlignet med situasjonen ved forrige forvaltningsrevisjon (2009).

Stillingen leder for informasjonssikkerhet hører til i IKT Konsern. Det er likevel først fra 2014 det står i oppdragsbrevet for IKT Konsern at informasjonssikkerhet er et av ansvarsområdene for seksjonen. Leder for informasjonssikkerhet er nå i ledergruppen i IKT Konsern, og det blir i intervju gitt uttrykk for at dette er en mer hensiktsmessig organisering. Rapporteringen på informasjonssikkerhetsområdet går fra leder for informasjonssikkerhet til direktør for IKT Konsern, samt direktør for byrådsavdeling for finans, eiendom og eierskap og kommunaldirektør for byrådsleders avdeling.

Et av tiltakene i informasjonssikkerhetsstrategien var å styrke bemanningen innen informasjonssikkerhetsområdet. Dette har blitt besluttet i 2014, og fra januar 2015 er det ansatt en person innenfor informasjonssikkerhetsområdet som rapporterer til leder for informasjonssikkerhet.

4.1.2.2 IKT Drift

IKT Drift har ansvar for informasjonssikkerhet i sine tjenester og prosesser. Spørsmål og forventninger knyttet til informasjonssikkerhet fra IKT Konsern kanaliseres primært gjennom informasjonssikkerhetsansvarlig i IKT Konsern til operativt sikkerhetsansvarlig i IKT Drift.

IKT Drift har utviklet et eget styringssystem for informasjonssikkerhet hvor overordnede føringer, interne instrukser, driftsdokumentasjon mv. er samlet i et eget dokument. Det går fram av intervju at IKT Drift legger til grunn NS-ISO/IEC 27001 og ISFs Standard of Good Practice (SoGP) for sitt arbeid med informasjonssikkerhet.

Det har blitt gjennomført en ekstern IT-revisjon i IKT Drift i 2012. Et av temaene for revisjonen er IKT Drifts arbeid med informasjonssikkerhet. Revisjonen påpeker bl.a. at det er manglende kultur for å gjennomføre systematiske risikovurderinger, manglende ledelsesgjennomgang og uklare ansvarsforhold knyttet til informasjonssikkerhet. Det går videre fram at revisor mener Bergen kommune «bør søke å etablere en omforent sikkerhetsarkitektur med tilhørende akseptabelt risikonivå som eies av IKT Konsern, men forvaltes av en samling av IKT Drift, byrådsavdelinger og IKT Konsern». Revisor viser til at slik samhandling er søkt løst gjennom forum som IT-Sikkerhetsforum, men at revisor «ikke [har] sett spor eller aktivitet for at denne samhandlingen faktisk blir utført som tiltenkt».

Det går fram av intervju at krav til informasjonssikkerhet i dag inngår på et overordnet nivå i driftstjenesteavtalen med IKT Drift, men det er ikke en egen driftsavtale med konkrete krav og rapportering for sikkerhetsområdet.

4.1.2.3 IKT-koordinatorer og informasjonssikkerhetsforum

Det er tilknyttet IKT-koordinatorer til hver byrådsavdeling. IKT-koordinatorene har et overordnet ansvar for koordinering av IKT innen en eller flere byrådsavdelinger. I følge strategien har koordinatorene «et overordnet ansvar for oppfølging av styringssystem for informasjonssikkerhet innen sine respektive områder».

På det taktiske nivået i informasjonssikkerhetsstrategien er det plassert et «informasjonssikkerhetsforum». Strategien beskriver det som ISA (leder for informasjonssikkerhet) sitt operative organ. Forumet skal bl.a. bestå av IKT-koordinatorer for de enkelte byrådsavdelingene og operativt sikkerhetsansvarlig (i IKT Drift), og skal ha som ansvar å utarbeide planer og forberede rapporter til strategisk nivå.

I intervju går det fram at informasjonssikkerhetsforum ikke lenger møtes. Det går imidlertid fram at informasjonssikkerhet tas opp som tema under IKT Samhandlingsmøtene dersom det er behov for dette. Disse møtene holdes fast hver annen måned.

Leder for informasjonssikkerhet forklarer at bakgrunnen for at dette forumet ikke lenger møtes er at det ikke har fungert så bra som forventet.

Et av de overordnede tiltakene i gjeldende informasjonssikkerhetsstrategi er en «konkret tiltaksplan innen styringssystemets enkelte segmenter utarbeides og revideres årlig». Dette har ikke blitt gjennomført. Leder for informasjonssikkerhet forklarer at han hadde sett for seg at arbeidet med tiltaksplaner skulle baseres på at IKT-koordinatorene skulle være kontaktpunktene. Dette har ikke fungert etter intensjonen. Det var vanskelig for koordinatorene å både ta den kreative rollen knyttet til å utvikle bruk av IKT og samtidig diskutere sikkerhet. I stedet for å utarbeide slike tiltaksplaner har leder for informasjonssikkerhet valgt å fokusere på klassifiseringsprosjektet (se 4.1.3 over). Han forklarer at man gjennom ny informasjonssikkerhetsstrategi trolig vil erstatte forumet med et nytt informasjonssikkerhetsråd (se 4.1.7).

Videre ser leder for informasjonssikkerhet for seg at man i større grad vil ha driftsmøter med IKT Drift, med utgangspunkt i driftsavtalen som regulerer arbeidet til IKT Drift. Han ønsker å ha to faste møter:

ett med helpdesk, der man går gjennom sikkerhetshendelser, og ett møte med lederne i IKT Drift for å få informasjon om nettverk, servere, og andre tekniske forhold.

IKT Konsern har ansvar for å ta imot politiske signal og omsetter disse til kommunens strategiske mål på IKT området. Kommunaldirektør ved Byrådsavdeling for finans, eiendom og eierskap forklarer at IKT Konsern derfor har en rolle som premissgiver for IKT og informasjonssikkerhet. I byrådssak 1058/14 ble det besluttet at IKT Drift skal beholdes som en etat i kommunen. Her går det fram at IKT Drift er organisert med utgangspunkt i en bestiller-/utførerorganisering, og at IKT Konsern «eier» oppdragsavtalen med IKT Drift. I byrådssaken påpekes det at vurderinger sikkerhet og sårbarhet er en viktig forutsetning for valget av organisering.

Det går frem i intervjuer at samarbeidet mellom IKT Konsern og IKT Drift knyttet til informasjonssikkerhet er bedret i løpet av de siste fem årene. Direktør for IKT Konsern forklarer likevel at det fremdeles er en vei å gå. Spesielt er det utfordringer knyttet til å avklare arbeidsdelingen av hva IKT Drift skal foreta på eget initiativ, og hva som skal bestilles fra IKT Konsern, og rapporteres til leder for informasjonssikkerhet.

4.1.2.4 Systemeiere og -koordinatorer

«Systemeier» er en sentral rolle knyttet til IKT og informasjonssikkerhet i kommunen. Systemeier er eier av informasjonen i systemene. Alle systemene som benyttes i Bergen kommune skal ha tilordnet en systemeier. Noen systemer er konsernovergripende og vil ha felles systemeier. I konsernovergripende konsern, bl.a. system som Portal, BKsak og fellesdata, er ofte systemeier tilhørende i IKT Konsern. For de systemene som ligger i de enkelte byrådsavdelingene er ansvaret fordelt forskjellig. I byrådsavdeling for barnehage og skole er det for eksempel fagavdelingen som har ansvar, mens det er kommunaldirektør som har systemansvar for alle fagsystemene i byrådsavdeling for helse og omsorg.

I tillegg til systemeiere skal det også være utpekt systemkoordinatorer for systemene. Systemkoordinator er det som også kalles «ressursperson». Dette er en administratorrolle i systemet.

Det er i dag tilgjengelig et dokument på intranett som beskriver ansvar og oppgaver for systemeiere. Dette omfatter:

- kartlegging og klassifisering av informasjon,
- risikovurdering
- rapportering av hendelser med betydning for informasjonssikkerhet
- å ha oversikt over om informasjonen behandles på grunnlag av hjemmel i lovverket (og om det er meldt eller søkt konsesjon til Datatilsynet).
- beredskapsplanlegging

I spørreundersøkelsen som ble gjennomført i forbindelse med revisjonen var det 11 respondenter som oppgav at de er systemeiere for ett eller flere systemer. Disse ble stilt spørsmålet: «I hvilken grad er det klart for deg hvilket ansvar som følger med det å være systemeier?» Fem svarte at det i stor eller svært stor grad var klart, fire svarte at det i noen grad var klart og to svarte at det i liten og svært liten grad var klart.

IKT Konsern er i ferd med å utarbeide et rolledokument. Dette dokumentet går bl.a. gjennom rollen som systemeier, der ansvaret konkretiseres i større grad enn tidligere. Rolledokumentet vil være grunnlaget for å stille mer krav til systemeier og koordinator. Leder for informasjonssikkerhet forklarer at det i dag er det en del tilfeldigheter knyttet til systemeierskapet. I en avdeling kan systemeier ikke være annet enn en proforma-rolle, mens kunnskapen om informasjonen i systemene ligger hos andre. Leder for informasjonssikkerhet mener det bør være mer konkret ansvar knyttet til den enkelte systemeier.

4.1.3 Systemoversikt og risikovurderinger

IKT Konsern har en oversikt over systemer og tjenester som er i bruk i kommunen. Oversikten gir en kort beskrivelse av formålet med systemet og hvem som er «systemeier».

Videre kartlegges det hvorvidt systemet inneholder personopplysninger eller andre taushetsbelagte opplysninger. Det registreres hvem som er den daglige behandlingsansvarlige, hvilket hjemmelsgrunnlag man har for å behandle disse opplysningene og om det er sendt melding eller om man har mottatt konsesjon fra Datatilsynet for behandling av disse opplysningen. Disse feltene er dog i varierende grad fylt ut, og versjonen av oversikten mottatt til denne revisjonen inneholder eksempelvis ingen informasjon om «Melding eller Konsesjon».

Arbeidet med kartlegging av systemer er forankret i informasjonssikkerhetsstrategien som et tiltak: «Kartlegge og klassifisere alle vesentlige informasjonsbehandlinger med hensyn til sikkerhetskrav».

Leder for informasjonssikkerhet forteller i intervju at han har fått gått lite i dybden på de enkelte system i oversikten, men at han til en viss grad fått kvalitetssikret at listen er komplett (inneholder alle systemene som er i bruk). I den grad han har gått i dybden på noen av systemene har dette hittil vært ad-hoc og hendelsesbasert. I det videre arbeidet med systemoversikten vil det imidlertid legges til grunn et mer systematisk internkontrollarbeid, basert på avdelingsvis gjennomgang av de enkelte systemene for hver byrådsavdeling være helt sentralt.

Prosjektet «Klassifisering av informasjonssystemer i Bergen kommune», som har gått fra september 2013 til januar 2015, har hatt som målsetning å kartlegge, klassifisere og prioritere de viktigste av kommunens informasjonssystemer. Leder for informasjonssikkerhet har vært prosjekteier- og deltaker i prosjektet, og kommunaldirektørene ved Byrådsavdeling for byutvikling, klima og miljø (BBKM), Byrådsavdeling for helse og omsorg (BHO), Byrådsleders kontor (BLED) og Byrådsavdeling for finans, eiendom og eierskap (BFEE) har vært styringsgruppe.
Arbeidet som er gjennomført omfatter:

- kvalitetssikring av oversikten over informasjonssystemer
- identifisering og klassifisering av informasjonssystemer
- gjennomføring av scenariobaserte konsekvens- og risikovurderinger
- videreutvikling av risikovurderingsmetodikk

På bakgrunn av prosjektet fremmes det også forslag til tiltak for å understøtte drift av mest kritiske systemene på en bedre måte enn i dag.

Klassifiseringsprosjektet er knyttet til den overordnete ROS-analysen for Bergen kommune, som leder for informasjonssikkerhet har deltatt i arbeidet med. Klassifiseringsprosjektet skal fungere som en nivå-2-ROS innen IKT og informasjonssikkerhet. I klassifiseringen av informasjonssystemene har man lagt til grunn kriterier som plasserer systemer i kategorier fra «lav» til «kritisk». Disse kategoriene er laget på basis av KOBI-rapporten[6], og i prosjektet har man hatt som utgangspunkt at kriteriene kan kobles til den overordnete konsekvensmatrisen for ROS-arbeidet i Bergen kommune.

Leder for informasjonssikkerhet forklarer at han har etablert et godt samarbeid med seksjon for samfunnssikkerhet og beredskap. Han har blant annet vært med på å utarbeide kommunens del av øvelse Bjørgvin, arbeidet opp mot overordnet ROS og har et godt samarbeid med beredskapssjefen i forbindelse med klassifiseringsprosjektet, hvor beredskapssjefen blant annet har deltatt på en del av møtene med kommunaldirektørene.

Informasjonssikkerhetsansvarlig har også begynt å jobbe opp mot Vann- og avløpsetaten i Bergen kommune, og har i denne sammenhengen også hatt dialog med VAV i Oslo om informasjonssikkerhetsspørsmål.

Når det gjelder risikovurderinger av systemer, legger gjeldende rutiner for informasjonssikkerhet i utgangspunktet ansvaret ut til de enkelte avdelinger og enheter. I funksjonsbeskrivelsen for rollen som systemeier som ligger på intranett går det fram at «for å vite om informasjonen man behandler er

[6] Koordineringsutvalg for informasjonssikkerhet (KIS): "Klassifisering Og Beskyttelse av Informasjon", 2008.

tilstrekkelig sikret, må man gjennomføre en risikovurdering.» Rutinen gir ikke informasjon om hvilke maler for risikovurdering som skal brukes, hvem som kan kontaktes for assistanse med dette arbeidet eller hvilke akseptkriterier risikovurderingen skal gjøres opp mot.

De elleve respondentene i undersøkelsen som oppgav at de er systemeiere for ett eller flere systemer ble stilt spørsmål om det er gjort risikovurdering for systemet(ene) de er systemeier for. Tre svarte «ja, men ikke for alle systemer», mens resten svarte «nei» eller «vet ikke». På oppfølgingsspørsmål om hvordan risikovurdering har blitt gjennomført, svarte en at det har blitt gjennomført gjennom en risikomodul i kvalitetssystemet og en svarte at det ikke var skriftliggjort (den siste svarte ikke på oppfølgingsspørsmålet).

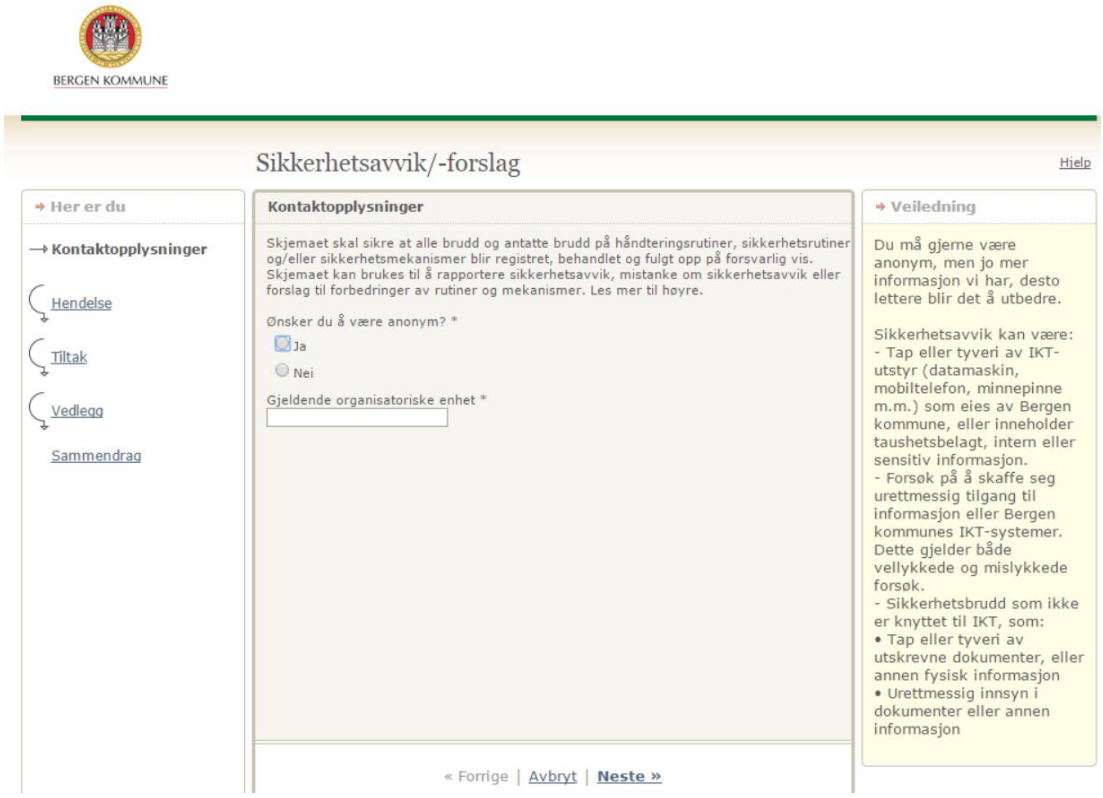
Både leder for informasjonssikkerhet (IKT Konsern) og operativt sikkerhetsansvarlig (IKT Drift) påpeker i intervju at det i for liten grad har blitt gjennomført risikovurderinger knyttet til informasjonssikkerhet.

I det overordnede ROS-arbeidet har det blitt gitt et utgangspunkt for akseptkriterier (definisjoner av «akseptabel», «tolerabel» og «uakseptabel» risiko), med henvisninger til hvordan man skal klassifisere av sannsynlighetsberegning og konsekvens av uønsket hendelse.[7] Leder for informasjonssikkerhet forklarer at risikovurderingene på informasjonssikkerhetsområdet vil knyttes til akseptkriteriene, men at dette er et arbeid man bare så vidt har startet med. Det har blitt utarbeidet utkast for akseptkriterier for risikovurderinger av informasjonssikkerhet, samt et verktøy for risikovurderinger i Excel-format. Disse dokumentene er likevel ikke gjort allment tilgjengelige på intranett/BKDOK.

4.1.4 Avvikshåndtering

For registrering av avviksmeldinger knyttet til informasjonssikkerhet er det gjort tilgjengelig et skjema på intranett. Det går fram av skjemaet at det kan brukes til å rapportere sikkerhetsavvik, mistanke om sikkerhetsavvik eller forslag til forbedringer av rutiner og mekanismer (se figur 2).

Figur 2 Skjema for sikkerhetsavvik



[7] Jf. Byrådssak 123/13

Leder for informasjonssikkerhet varsles automatisk om avvik meldt i skjemaet via e-post. Tidligere skjedde registreringen gjennom meldinger til eget e-postmottak, men nå registreres også avvik i BK-sak (og leder for informasjonssikkerhet får i tillegg varsel på e-post). Leder for informasjonssikkerhet anslår at det er registrert ca. 120 avvik totalt gjennom de årene avviksregistreringen har vært aktiv, og han mener det per i dag registreres alt for få avvik. Det er ikke alle avvikene som registreres gjennom dette systemet. Mange avvik meldes gjerne mer uformelt, muntlig, enten direkte eller over telefon. Leder for informasjonssikkerhet forklarer at innholdet i avvikene er sprikende. Det er alt fra ønske om å stenge Facebook i arbeidstiden, til passordproblemer og mer alvorlige tekniske sikkerhetsproblemer med ulike løsninger.

Leder for informasjonssikkerhet forklarer i intervju at han ikke har hatt anledning til å prioritere formalisering av avviksbehandling høyt frem til i dag. Avvikshåndtering, som internkontrollaktiviteter for øvrig, vil være en av oppgavene som prioriteres høyre når avdelingen nå har blitt tilført ressurser.

I tillegg til avvikene som meldes til leder for informasjonssikkerhet er det en lang rekke hendelser som registreres i helpdesk, og enkelte av disse kan være sikkerhetsrelaterte. Det har også forekommet kjente sikkerhetsbrudd som har karakter av "hacking"-relaterte hendelser, informasjonslekkasje mv. IKT Drift har instruks og prosess for avvikshåndtering i styringssystemet. Det går frem av intervju at hendelsene som IKT Drift håndterer primært har vært knyttet til tilgjengelighet til systemer/data, og i mindre grad konfidensialitet eller integritet av data i systemene.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, svarer 62 % at respondentene at de *ikke* kjenner til rutinene for å melde avvik knyttet til informasjonssikkerhet. På samme spørsmål var det i 2009 83 % som svarte de ikke kjente til rutinene (se tabell 1 under).

Tabell 1: Kjenner du rutinene for å melde avvik knyttet til informasjonssikkerhet?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
Ja	28,6 %	34,5 %	15,4 %	43,1 %	38,1 %	12,2 %	22,4 %	13,7 %	10,0 %	16,9 %
Nei	71,4 %	65,5 %	84,6 %	56,9 %	61,9 %	87,8 %	77,6 %	86,3 %	90,0 %	83,1 %
Ant all	14	84	13	109	331	74	152	131	10	367

4.1.5 Sikkerhet hos kommunikasjonspartnere og leverandører

Leder for informasjonssikkerhet forklarer at han har jobbet mye med databehandleravtaler[8], overfor Microsoft, It's Learning og en rekke andre leverandører. Bergen kommune har lenge hatt en standardisert databehandleravtale som er gjort tilgjengelig for bruk på informasjonssikkerhetssidene på intranett.

Sikkerhet overfor samarbeidspartnere er et særlig aktuelt tema i forbindelse med anskaffelser av IT-utstyr og -tjenester. Leder for informasjonssikkerhet opplever at mange leverandører har liten forståelse for krav og standarder på informasjonssikkerhetsområdet. Bergen kommune jobber sammen med andre instanser, gjennom bl.a. K10, KommIT (nettverk for samarbeid om IKT mellom kommuner), og Difi, om standardisering av krav til leverandører. Det påpekes i intervju at samarbeid med disse aktørene er viktig både for å finne fram til nye, effektive IKT-løsninger, men også å dele kunnskap om informasjonssikkerhet med andre aktører.

Direktør for IKT Konsern mener at kommunen har blitt flinkere på å innarbeide informasjonssikkerhets-perspektiver i sitt arbeid. Dette gjelder for eksempel praksis for å sikre at krav til informasjonssikkerhet, i form av risikovurderinger og sikkerhetsinformasjon, er på plass når man skal kjøpe inn nye produkter/løsninger.

[8] En virksomhet som behandler data på vegne av en annen virksomhet er ihht. regelverket en «databehandler». Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Dette reguleres av personopplysningsloven § 13, jf. § 15.

I denne sammenhengen reviderer leder for informasjonssikkerhet databehandleravtalen, bl.a. for å gjøre den mer tydelig i forhold til minstekravene til Datatilsynet, og på grunnlag av dette kunne utlede et sett med mer konkrete standardkrav til leverandører.

I intervju blir det forklart at IKT Drift alltid sjekker at det foreligger et rettmessig grunnlag og databehandleravtale dersom man skal utlevere data. I tillegg må eksterne konsulenter undertegne egen taushetserklæring.

4.1.6 Oppfølging av informasjonssikkerheten

Et av tiltakene i informasjonssikkerhetsstrategien er å foreta jevnlige sikkerhetsrevisjoner: Dette har ifølge intervju ikke blitt gjennomført annet enn på ad-hoc-basis. Sikkerhetsrevisjoner vil bli prioritert i forbindelse med at det har blitt ansatt en ny ressurs på informasjonssikkerhetsområdet i IKT konsern.

Det er ikke utarbeidet en rutine for «Ledelsens gjennomgang» av informasjonssikkerhet i Bergen kommune. Leder for informasjonssikkerhet påpeker at det er en god kommunikasjon med kommuneledelsen om informasjonssikkerhet, og at det er en klar ledelsesinvolvering av kommunaldirektører i informasjonssikkerhetsspørsmål gjennom møter på jevnlig basis mellom ledelsen i IKT Konsern og kommunaldirektørnivået.

4.1.7 Utrulling av styrings- og internkontrollsystem

Det går fram av intervju at leder for informasjonssikkerhet har satt i gang et arbeid med å samle rutiner og prosedyrer i et felles system, «IS-håndboken». Målet med dette arbeidet er å kunne gi et formelt overbygg for et felles styringssystem for informasjonssikkerhet.

Et av tiltakene i informasjonssikkerhetsstrategien har vært å etablere et elektronisk støttesystem «for å ivareta styrings- og internkontrollsystem for informasjonssikkerhet og andre områder med tilsvarende behov, som HMS-arbeidet». Leder for informasjonssikkerhet har samarbeidet med fagpersoner i kommunen som arbeider med HMS om å få på plass et elektronisk kvalitetssystem for dette formålet, men man har ikke fått aksept for å utvikle et slik system. Leder for informasjonssikkerhet forklarer i intervju at styrings- og internkontrollsystemet for informasjonssikkerhet i stedet vil publiseres på Bergen kommunes nye intranettløsning «Allmenningen».

Leder for informasjonssikkerhet forklarer at håndboken er bygd opp primært med utgangspunkt i ISO/IEC 27000-serien, men at det også «løselig» er bygd opp på grunnlag av Norm for informasjonssikkerhet. Leder for i viser til at ISO/IEC 27000 er en naturlig standard å velge med utgangspunkt i eForvaltningsforskriftens krav (§ 15) om at internkontrollsystemene skal basere seg på anerkjente standarder for styringssystem.

Strukturen i håndboken er bygd opp med en mappestruktur som omfatter hvilken overordnet prosess prosedyrene hører til («styring», «gjennomføring», «kontroll»), og er videre delt inn i mapper for ulike temaer innenfor hver av de overordnede prosessene. Dokumentene som skal legges ut på BKDOK skal også samles i et eget dokument, organisert med kapitler tilsvarende mappestrukturen for håndboken i BKDOK.

I intervju peker leder for informasjonssikkerhet på at det er en forutsetning at lederne i de ulike byråds-avdelingene har forståelse for behovet for et slikt system, for at innføringen skal være vellykket. Han gir uttrykk for at denne forankringen er i ferd med å komme på plass.

Informasjonssikkerhetsstrategien som er vedtatt har vært gjeldende fram til 2014. Ny strategi er ikke utarbeidet p.t. (februar 2015). Leder for informasjonssikkerhet, som har ansvar for å utarbeide utkast til strategien, peker i intervju på enkelte punkter hvor strategien vil endres fra den forrige:

- Informasjonsverdi og -klassifisering blir mer vesentlig
- Risikostyring, avvikshåndtering og beredskapsarbeid vil vektlegges mer
- Roller og ansvar vil endres i samsvar med ny organisering som IKT konsern er i ferd med å utvikle

- IKT-koordinatorer vil få en mindre fremtredende rolle, og sikkerhetsforum vil erstattes med et «sikkerhetsråd" bestående av beredskapssjef, informasjonssikkerhetsansvarlig og operativt sikkerhetsansvarlig i IKT Drift.

4.1.7.1 Styringssystem for informasjonssikkerhet innen helseområdet

Byrådsavdeling for helse- og omsorg (BHO) og byrådsavdeling for sosial, bolig og områdesatsing (BSBO) har en egen IKT-koordinator som også fungerer som informasjonssikkerhetskoordinator. Leder for informasjonssikkerhet i Bergen kommune forklarer i intervju at informasjonssikkerhetskoordinatoren arbeider godt på dette området med sin byrådsavdeling. Derfor har heller ikke leder for informasjonssikkerhet prioritert å jobbe mer inngående med dette området.

BHO og BSBOs arbeid med informasjonssikkerhet tar utgangspunkt i Norm for informasjonssikkerhet. IKT-koordinator ved byrådsavdelingene har fått maler fra leder for informasjonssikkerhet for å bruke som utgangspunkt i systemet.

Byrådsavdelingen har en egen systemoversikt som gir informasjon om hvilke systemer som behandler personopplysninger, og hvorvidt det er meldeplikt/konsesjonsplikt i disse systemene. I BHO og BSBO har man også utarbeidet dokumentasjon av rutiner ol. knyttet til de ulike fagsystemene (bl.a. Familia, Profil og Socio). Disse er tilgjengelige i BKDOK. Noen av rutinene omhandler kontroller/tiltak for å bedre informasjonssikkerhet, f.eks. autorisasjoner og tilganger. Det gjennomføres risikovurderinger i forbindelse med nye systemer eller større systemendringer. Disse risikovurderingene gjøres av IKT Drift, men IKT-koordinator bidrar inn i disse.

Styringssystem for informasjonssikkerhet var et tema i Norsk helsenetts eksterne gjennomgang av informasjonssikkerheten i 2012, der de vurderte om Bergen kommune oppfyller kravene til Normen. I sammendraget fra revisjonsrapporten fra Norsk helsenett går det fram følgende:

> *Hovedinntrykket er at Bergen kommune har god styring på informasjonsbehandlingen sin og sikkerheten i forbindelse med denne. På revisjonstidspunkt må vi dog bemerke som et forholdsvis alvorlig avvik at overordnet styringssystem for informasjonssikkerhet mangler. Vi er av den mening at dette må på plass før 2014 som planlagt i dag.*

I tilknytning til dette går det fram av rapporten at revisjonsgruppen fra Norsk helsenett fikk forelagt et utkast til innhold i dette styringssystemet. Norsk helsenett skriver:

> *[Styringssystemet] har etter vår mening en så stor ferdiggrad, at en godt kan sette flere rutiner i verk i god tid før 2014. Vi tenker i denne sammenheng på avvikshåndtering, risikostyring, sikkerhetsrevisjon og ledelsens gjennomgang.*

Det også fram at revisjonen «*forstår med tilfredshet at Normen vil bli kravdokument for hele kommunen i tråd med ny strategi for informasjonssikkerhet».*

Leder for informasjonssikkerhet oppgir i intervju at arbeidet med dagens overordnede styringssystem «kun løselig» er basert på normen (jf. 4.1.7). Han forklarer at man har funnet at man vil gå vekk fra å legge normen til grunn for styringssystemet, og påpeker at normen er innrettet for å sikre sensitive helseopplysninger. For de delene av virksomheten som er omfattet av Normen, vil man følge kravene, men for store deler av den kommunale virksomheten er det ikke hensiktsmessig å legge til grunn et slikt sikkerhetsnivå.

4.2 Opplæring og kjennskap til informasjonssikkerhet

4.2.1 Opplæringsmateriell og -tiltak

De ansatte har tilgang til ulike instrukser og retningslinjer i BKDOK, bl.a.

- Informasjonssikkerhetsstrategi 2011-2014
- Felles brukerinstruks IKT
- Overordnet passordinstruks for Bergen kommune
- Retningslinjer for internettbaserte tjenester

Leder for informasjonssikkerhet forklarer at han har arbeidet kontinuerlig med å oppdatere instrukser og retningslinjer. Samtidig forklarer han at han ikke har mulighet til å gå ut og informere organisasjonen på en effektiv måte når det skjer nye endringer, og at dette kan være en utfordring.

Status for tiltakene som er vedtatt i informasjonssikkerhetsstrategien knyttet til bevisstgjøring og sikkerhetskultur (se 4.1.1 over) er

1. *Integrere grunnleggende instrukser for sluttbrukere i personal- og arbeidsreglementet:*
   Det har fra før informasjonssikkerhetsstrategien ble vedtatt vært et avsnitt i informasjonssikkerhet i etisk standard for Bergen kommune. Leder for informasjonssikkerhet forklarer at han har kommet med innspill til HR-avdelingen for å integrere instrukser i reglementet, men at disse har ikke blitt innarbeidet.

2. *Standardisere krav til kartlegging, klassifisering, risikovurdering og avvikshåndtering:*
   Overordnede akseptkriterier for risikovurderinger i Bergen kommune er vedtatt. IKT konsern har med utgangspunkt i disse startet et arbeid med å lage utkast til akseptkriterier for risikovurderinger av informasjonssikkerhet, samt verktøy for risikovurderinger. Dette arbeidet er ikke ferdigstilt, og dokumentene er ikke tilgjengeliggjort (se 4.1.3 over).

3. *Erstatte dagens fornying av IT-sikkerhetserklæring med grunnleggende e-læring for informasjonssikkerhet:*
   Leder for informasjonssikkerhet har gjort om IT-sikkerhetserklæringen til «Felles brukerinstruks» og har lenge hatt et ønske om å gjøre instruksen e-læringsbasert og da med en test på at man har lest og forstått innholdet før man får lov til å fortsette å benytte kommunens IKT-plattform. Per i dag har ikke kommunen et verktøy for utvikling av e-læringsopplegg, men dette er noe HR arbeider med.

4. *Etablere styringskort for informasjonssikkerhet blant ledere.*
   Det er med i årsoppdraget til IKT konsern at informasjonssikkerhet skal inn i styringskort. Informasjonssikkerhet er innarbeidet i styringskortet til IKT Konsern, men er enda ikke på plass i styringskortet til alle andre ledere.

5. *Integrere kursmoduler for informasjonssikkerhet i eksisterende HR-kurs:*
   Leder for informasjonssikkerhet har integrert kursmoduler i HR. Han er med på en egen modul for kvalitetsstyring og internkontroll, i tillegg til at han er med på informasjonsdagene for nyansatte.

6. *Utarbeide og tilgjengeliggjøre en oversiktlig og informativ struktur for instrukser, retningslinjer og andre styrende dokumenter:*
   Retningslinjer og maler som er utviklet er samlet på intranett, og leder for informasjonssikkerhet har satt i gang et arbeid for å publisere en felles håndbok (jf. 4.1.7). Noen retningslinjer hvor leder for informasjonssikkerhet har bidratt ligger på andre sider, bl.a. informasjonsavdelingen.

7. *Informere organisasjonen om utviklingen i trusselbildet.*
   Leder for informasjonssikkerhet forklarer at det er behov for en mer hensiktsmessig involvering av linjeansvaret i informasjonssikkerhetsarbeidet. Han vurderer at organiseringen med sikkerhetsforum der IKT-koordinatorer møter ikke har vært optimal (se 0 over).

Leder for informasjonssikkerhet har utarbeidet både et heldagskurs for ledere i Bergen kommune og et foredrag med tittelen «IKT - Informasjon, Kommunikasjon og Teknokrati» (se pkt. 5 i listen over). I kurs og foredrag blir det bl.a. pekt på viktigheten av at ansatte og ledere må vite hvilken informasjon de behandler, hvilken informasjon de har tjenstlig behov for å behandle i sin arbeidshverdag, og la dette styre hvilken teknologi de tar i bruk og hvordan de bruker den. Leder for informasjonssikkerhet holder også foredrag på «Basiskurs for ledere» (lederopplæring) og på «Informasjonsdag for nyansatte».

Gjennom oktober, som er nasjonal sikkerhetsmåned, samarbeidet Bergen kommune i 2014 med Norsk senter for informasjonssikring og leverandøren JungleMap for tredje året på rad om en e-læringskampanje. Dette omfatter 10 leksjoner om ulike tema innen informasjonssikkerhet, og som også knytter disse temaene opp mot relevante styrende dokumenter, som felles brukerinstruks og ulike retningslinjer, om for eksempel digital kommunikasjon, sosiale medier og internettbaserte tjenester.

Direktør for IKT Konsern forklarer at det brukes mye krefter på opplæring på IT-området, og at man ser spor av opplæringen man har satt i gang knyttet til informasjonssikkerhet, blant annet gjennom økt etterspørsel etter tjenestene informasjonssikkerhetsmiljøet leverer.

I tillegg til de retningslinjene som gjelder sentralt for informasjonssikkerhet og personvern er det også utarbeidet retningslinjer som gjelder spesifikt innenfor de enkelte byrådsavdelingene. Dette er bl.a. gjort innenfor BSBO og BHO (se 4.1.7.1 over). I spørreundersøkelsen ble de som er resultatenhetsledere spurt om det er utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern i den enheten de er ledere for. 42 % av resultatenhetslederne svarte bekreftende på dette. Se tabell 2 under

Tabell 2: Er det utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern i den enheten du er resultatenhetsleder for?

	PPT	Skole	Barnevern	Annet	Total
Ja	100,0 %	60,0 %	0,0 %	28,6 %	42,1 %
Nei	0,0 %	40,0 %	100,0 %	57,1 %	47,4 %
Vet ikke	0,0 %	0,0 %	0,0 %	14,3 %	10,5 %
Antall	1	5	1	7	19

4.2.2 Ansattes kunnskap

I spørreundersøkelsen til de ansatte ble det stilt flere spørsmål knyttet til hvilke rutiner og retningslinjer respondentene har lest, og hvorvidt de er kjent med innholdet i disse. Svarene som ble oppgitt i undersøkelsen er gjengitt i tabeller i vedlegg 1 under.

Alle brukere i Bergen kommunes IT-systemer får årlig opp en melding der de må bekrefte at de har lest «felles brukerinstruks» (tidligere IT sikkerhetserklæring). I spørreundersøkelsen ble respondentene spurt om de har lest felles brukerinstruks. Det er 68 % av respondentene som bekrefter at de har lest instruksen. Til sammenligning var det i 2009 var det 82 % som oppgav at de hadde lest instruksen. Blant de som i 2014 bekrefter at de har lest instruksen er det 23 % som oppgir at de i stor eller svært stor grad husker innholdet i instruksen. Se tabell 10 og tabell 11.

Det er utarbeidet en overordnet retningslinje for behandling av personopplysninger i Bergen kommune. Blant respondentene i 2014 var det 50 % som oppgav at de hadde lest denne retningslinjen. Se tabell 13.

I 2014 ble også respondentene spurt om de vet hvor man finner rutiner og retningslinjer for informasjonssikkerhet på Bergen kommunes intranett. 73 % av respondentene svarte ja på dette spørsmålet. Se tabell 16.

Videre ble respondentene spurt om de har fått tilstrekkelig opplæring i hvordan IT-systemene de benytter skal brukes. På dette spørsmålet er det følgende svarfordeling (2009-tall i parentes):

- «Ja, opplæringen har vært tilstrekkelig»: 40 % (41 %)

- «Ja, men ikke i alle IT-systemene jeg bruker»: 22 % (28 %)
- «Nei, opplæringen kunne vært bedre»: 36 % (30 %)
- «Ikke aktuelt»: 2% (2 %)

Se tabell 18.

I spørreundersøkelsen fikk respondentene mulighet til å selv påpeke områder hvor Bergen kommune har et forbedringspotensial knyttet til informasjonssikkerhet. Flere av respondentene påpekte at det var forbedringspotensial knyttet til hvordan personopplysninger håndteres. Dette gjelder bl.a. personalopplysninger, opplysninger om brukere i sosial- og helsetjenesten og elevopplysninger. Særlig er det flere som påpeker at det er rom for forbedring i hvordan personopplysninger på papir oppbevares. Det påpekes også at det er viktig å gjennomgå rutiner knyttet til hvordan personopplysninger mellom ulike instanser deles, og at det er viktig å ha fokus på hvilken informasjon det er nødvendig å utveksle.

I tillegg er det flere som etterspør bedre opplæring knyttet til taushetsplikt, retningslinjer for informasjonssikkerhet og hvilke krav det er til å lagre og sende sensitiv informasjon elektronisk. I denne sammenhengen peker respondentene bl.a. på at det er viktig at enhetsledere tar ansvar for at alle ansatte har kunnskap om retningslinjene, Det foreslås bl.a. at dette er tema som kan tas opp på fagdager og personalmøter der mange er samlet.

5 Vurderinger

5.1 I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket knyttet til informasjonssikkerhet?

5.1.1 Er det innført rutiner og retningslinjer i samsvar med anbefalingene fra rapporten i 2009

Bergen kommune har satt i verk flere tiltak for å bedre informasjonssikkerheten i kommunen og tilfredsstille krav i lovverket etter forvaltningsrevisjonen som ble gjennomført i 2009. Revisjonen mener likevel at undersøkelsen viser at det fortsatt er flere forhold knyttet til informasjonssikkerhet som må forbedres for å sikre at informasjonssikkerheten i kommunen skal være tilfredsstillende.

Sentralt blant anbefalingene fra forvaltningsrevisjonsrapporten i 2009 var å etablere et informasjonssikkerhetssystem i samsvar med kravene i personopplysningsforskriften. I 2014 er status at kommunen har arbeidet med å utbedre flere av elementene i et slikt styringssystem.

Revisjonen viser at det på flere områder er gjort vesentlig forbedringer. Det er blant annet fastsatt en overordnet informasjonssikkerhetsstrategi, og det er i forhold til forrige revisjon etablert en bedre oversikt over hvilke systemer og elektroniske tjenester som er i bruk i kommunen. Gjennom klassifiseringsprosjektet har kommunen fått gjennomført en «nivå 2-ROS» med risikovurdering på utvalgte områder knyttet til informasjonssystemene i kommunen, og informasjonssikkerhet har inngått som en del av det overordnede ROS-arbeidet i kommunen. Revisjonen vil også trekke fram at kommunen har gjennomført et arbeid med rutiner og retningslinjer for informasjonssikkerhet for de delene av virksomheten som skal være knyttet til Norsk helsenett. Videre er det gjort et viktige arbeid for å bedre oversikten over sikkerhet hos leverandører gjennom databehandleravtaler og krav til informasjonssikkerhet i anskaffelsesprosesser.

På den annen side viser revisjonen at det på flere områder er mangler knyttet til kommunens styringssystem for informasjonssikkerhet. Revisjonen vurderer at følgende må regnes som vesentlige mangler ut fra de rutinene og retningslinjene som er gjeldende i dag:

- Det går ikke klart fram av systemoversikten hvilke systemer som behandler personopplysninger, og i hvilken grad disse er melde- eller konsesjonspliktige. Videre framstår det som uklart hvordan det er forventet at de ulike systemeierne skal gjennomføre risikovurderinger av sine systemer/tjenester. Dette er ikke i samsvar med krav i personopplysningsforskriften § 2-4.
- Det er ikke innført rutiner for sikkerhetsrevisjoner, og det har ikke blitt gjennomført sikkerhetsrevisjoner på annet enn ad hoc-basis. Dette er ikke i samsvar med krav i personopplysningsforskriften § 2-5.
- Det er ikke innført en rutine for «ledelsens gjennomgang» av informasjonssikkerhet. Status og tiltak for informasjonssikkerhet blir jevnlig rapportert og drøftet med kommunaldirektørnivået, men revisjonen vurderer at jevnlig (f.eks. årlig) ledelsesgjennomgang av sikkerhetsmål og strategi bør fastsettes i en rutine for å sikre oppfyllelse av personopplysningsforskriften § 2-4.[9]

Videre ønsker revisjonen å påpeke at selv om det er innført en rutine for avviksregistrering, blir det i liten grad meldt informasjonssikkerhetsavvik via denne kanalen. Spørreundersøkelsen som er gjennomført i forbindelse med revisjonen viser at det er under 40 % av respondentene som kjenner til hvor man skal registrere avvik knyttet til informasjonssikkerhet.

[9] Se bl.a. Datatilsynet: «Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer». SV-100:2000.

Revisjonen mener at en viktig forutsetning for å kunne lykkes i Bergen kommunes arbeid med informasjonssikkerhet er å sørge for en tydelig definisjon av roller og fordeling av oppgaver knyttet til de aktørene som har et ansvar for informasjonssikkerhet. Det går fram av undersøkelsen at samarbeid mellom IKT Konsern, byrådsavdelinger og IKT Drift har blitt forbedret på mange områder i løpet av de siste fem årene. Per i dag er det likevel områder hvor ansvar- og rollefordeling oppleves som uklar. Videre framgår det av revisjonen at systemeierne kommunen ikke i tilstrekkelig grad kjenner sine roller og oppgaver. Det er derfor etter revisjonens vurdering viktig å tydeliggjøre roller og ansvar i enda større grad enn i dag (se også 5.2 under).

Samlet sett mener revisjonen at ovennevnte forhold er vesentlige svakheter ved hvordan Bergen kommunes overordnede styringssystem per i dag fungerer, sett i forhold til kravene i personopplysningsforskriften kap. 2 og eForvaltningsforskriften § 15.

Flere av disse forbedringsområdene ble også påpekt i informasjonssikkerhetsstrategien (2011 – 2014), hvor det ble vedtatt flere relevante tiltak for å utvikle styringssystemet og innfri krav i regelverket. Vår gjennomgang viser at det er flere av tiltakene som ikke har blitt gjennomført, eller som har blitt vesentlig endret i den faktiske gjennomføringen. Dette gjelder bl.a. utarbeidelse av tiltaksplan for styringssystemets enkelte segmenter, etablere styringssystem med utgangspunkt i Norm for informasjonssikkerhet, å foreta jevnlige sikkerhetsrevisjoner, å etablere elektronisk støttesystem for internkontrollsystem, samt flere av tiltakene knyttet til instrukser, styringskort og informasjon under fokusområdet «bevisstgjøring» (se 4.2.1). Revisjonen mener at en av årsakene til dette, er at tiltakene har forutsatt flere spesialiserte ressurser for arbeid med informasjonssikkerhet enn det som har vært tilgjengelig. Videre er flere av tiltakene avhengig av høy prioritering av informasjonssikkerhet på tvers av byrådsavdelinger og fagområder. Til sist vil det være naturlig at nye problemstillinger og ny kunnskap dukker opp underveis i planprosessen, og at dette kan skape behov for å justere eller endre tiltakene i planen. Revisjonen mener at det ville være en fordel om strategien hadde stilt tydelige krav til frister, rapportering og eventuell rullering av tiltakene.

5.1.2 I hvilken grad er det gitt føringer for å sikre en helhetlig tilnærming til informasjonssikkerhet i kommunen?

For å svare på i hvilken grad det er gitt føringer for en helhetlig tilnærming til informasjonssikkerheten er det nødvendig å vurdere både bredden og systematikken av informasjonssikkerhetsarbeidet. Med *bredden* mener vi i hvilken grad informasjonssikkerhetsarbeidet – og det praktiske definisjonsområdet for informasjonssikkerhet i kommunen – er innrettet for å fange opp relevante risikoer innen ulike typer eller kategorier av informasjon. Med *systematikken* mener vi i hvilken grad det er lagt til rette et felles system for å håndtere informasjonssikkerhetsarbeidet på tvers av temaer, enheter og avdelinger.

Når det gjelder hvilke områder som inngår i informasjonssikkerhetsarbeidet, viser vår gjennomgang at Bergen kommune ikke baserer sin tilnærming til temaet gjennom en snever fortolking av informasjonssikkerhet som «vern om elektronisk lagrede personopplysninger». Et mer helhetlig perspektiv har blitt ivaretatt ved at oppmerksomheten i informasjonssikkerhetsarbeidet også har rettet seg mot bl.a. samfunnssikkerhet og vern av materielle verdier. Arbeidet med kartlegging av systemer som nylig er gjennomført, viser at kommunen har lagt til rette for et helhetlig og bredt perspektiv på informasjonsverdi og –sikkerhet.

Når det gjelder det formelle systemet som er lagt til grunn for arbeidet vurderer revisjonen at Bergen kommune – på grunn av manglene i det overordnede styringssystemet (se 5.1.1 over) – ikke har en tilstrekkelig helhetlig tilnærming til informasjonssikkerhet. Mangel på tydelige sentrale retningslinjer vil øke risikoen for at praksis for informasjonssikkerhetsarbeidet varierer mellom avdelinger og enheter, at behandlingsansvarlige ikke får tilstrekkelig oversikt over praksis for informasjonssikkerhet innen sitt ansvarsområde og at sentralt vedtatte mål for informasjonssikkerhet i kommunen ikke nås.

5.2 I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet tydeliggjort?

I strategi for informasjonssikkerhet blir det fordelt ansvar gjennom hele organisasjonen for roller og oppgaver knyttet til informasjonssikkerhet.

I praksis er det noen av rollene som er nevnt i informasjonssikkerhetsstrategien som ikke per i dag er virksomme. Dette gjelder bl.a. informasjonssikkerhetsrådet og informasjonssikkerhetsforum. Begge disse er tillagt en sentral rolle i informasjonssikkerhetsstrategien, men i dag brukes andre, eksisterende fora for å håndtere informasjonssikkerhetsspørsmål. Revisjonen mener det kan være uheldig at en slik endring av roller og oppgaver ikke er forankret i et formelt, skriftliggjort vedtak.

Revisjonen vurderer at ansvar og oppgavefordeling på et overordnet nivå innenfor Byrådsavdeling for finans, eiendom og eierskap i dag er tydeliggjort, bl.a. gjennom byrådsvedtak om organisering av IKT Drift. Etter det revisjonen har fått opplyst vil ny informasjonssikkerhetsstrategi fastsette ansvars- og rollefordeling i samsvar med oppgave- og rollebeskrivelser som er under utarbeidelse i IKT Konsern.

Når det gjelder ansvar og oppgaver knyttet til informasjonssikkerhet på det strategien omtaler som «operasjonelt nivå», vurderer revisjonen at dette i dag ikke er tilstrekkelig tydelig. Systemeier er tillagt en rekke sentrale oppgaver knyttet til kartlegging, klassifisering, risikovurdering og beredskapsplanlegging, men det går etter revisjonens vurdering ikke tilstrekkelig tydelig fram av retningslinjene hvordan de som har rollen som systemeier skal ivareta dette ansvaret. I spørreundersøkelsen var det også flere av de som oppgav at de er systemeiere som ga uttrykk for at det ikke var fullt ut klart hva ansvaret som systemeier innebærer. Revisjonen mener at det er viktig å gi systemeiere så tydelige og fullstendige instrukser som mulig, da disse er satt til å ivareta oppgaver som fordrer relativt god innsikt i informasjonssikkerhetsfaglige termer og problemstillinger.

5.3 I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Et av tiltakene fra forvaltningsrevisjonsrapporten som ble gjennomført i 2009 var å *sørge for at rutiner og retningslinjer knyttet til informasjonssikkerhet […] blir tilstrekkelig implementert på alle nivå i kommunen, samt at medarbeiderne har nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner.*

Revisjonen vurderer at Bergen kommune fremdeles har et klart forbedringspotensial når det gjelder de ansattes kjennskap til sentrale retningslinjer og instrukser. Under 70 % av respondentene i spørreundersøkelsen svarte bekreftende på at de hadde lest «felles «brukerinstruks». Dette er en instruks som alle ansatte må lese for å få tilgang til Bergen kommunes IT-systemer, og som de må bekrefte årlig at de har lest. Bare 50 % av respondentene har lest overordnet retningslinje for behandling av personopplysninger.

Når det gjelder «lokale» rutiner og retningslinjer, går det fram at det er utarbeidet slike i de enkelte enheter, bl.a. innenfor PPT og skole. Det er også flere respondenter som i undersøkelsen påpeker at det er forbedringspotensial knyttet til rutiner for å håndtere ulike typer personopplysninger i kommunen.

En av årsakene til at mange av de ansatte ikke har lest sentrale instrukser og retningslinjer kan være at det er uklart for mange hvor man finner rutinene. Det er 27 % av respondentene som ikke vet hvor de finner rutiner og retningslinjer for informasjonssikkerhet på Bergen kommunes intranett. Det er også et flertall av respondentene som oppgir at de savner opplæring i IT-systemene de bruker. Flere respondenter etterspør bedre opplæring knyttet til oppbevaring av personopplysninger, taushetsplikt, retningslinjer for informasjonssikkerhet og krav knyttet til å sende og lagre sensitiv informasjon. Revisjonen mener dette viser at man ikke har tilstrekkelig kjennskap til retningslinjer og rutiner per i dag, og at Bergen kommune bør finne effektive tiltak for å gi ansatte tilstrekkelig kunnskap om disse temaene.

6 Anbefalinger

IKT Konsern er nå i gang med et arbeid for å utbedre og konsolidere et styringssystem for informasjonssikkerhet. Dette arbeidet vil stå sentralt i det videre arbeidet med informasjonssikkerhet i kommunen. Med bakgrunn i funnene i denne forvaltningsrevisjonen anbefaler revisjonen at Bergen kommune vurderer å gjennomføre følgende tiltak:

1. Utbedre de elementene i styringssystemet hvor det er påpekt mangler, med særlig vekt på
   a) Risikovurderinger
   b) Sikkerhetsrevisjoner
   c) Avvikshåndtering
   d) Ledelsens gjennomgang
2. Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.
3. Sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert og sikre at alle ansatte kjenner til hvor man finner rutinene.
4. Ved utarbeidelse av ny strategi for informasjonssikkerhet, fastsette krav til oppfølging av og rapportering på gjennomføring av tiltak, samt eventuell rullering av planer og tiltak.

Vedlegg 1 Svar fra spørreundersøkelsen

Tabell 3: Vet du hvem i kommunen du skal kontakte dersom du har spørsmål knyttet til informasjonssikkerhet og behandling av personopplysninger?

	2014			2009		
	Resultat-enhetsledere	Andre	Total	Resultat-enhetsledere	Andre	Total
Ja	61,1 %	38,6 %	39,6 %	75,0 %	29,9 %	34,3 %
Nei	38,9 %	61,4 %	60,4 %	25,0 %	70,1 %	65,7 %
Antall	18	308	328	36	331	367

Tabell 4: Hvem ville du kontaktet dersom du har spørsmål knyttet til informasjonssikkerhet? (Du kan krysse av for flere alternativer.)

	2014
Min nærmeste leder	82,2 %
Kollega/kollegaer med kunnskap om temaet	20,9 %
Systemeier (dersom spørsmålet gjelder et konkret system/tjeneste)	18,6 %
Systemkoordinator (dersom spørsmålet gjelder et konkret system/tjeneste)	27,1 %
Informasjonssikkerhetsansvarlig/leder for informasjonssikkerhet i Bergen kommune	47,3 %
Helpdesk	45,0 %
IKT Drift	31,0 %
Datatilsynet	3,1 %
Andre	3,9 %
Antall	129,00

Tabell 5: Hvem ville du kontaktet dersom du har spørsmål knyttet til informasjonssikkerhet? (Du kan krysse av for flere alternativer.)

	2014	2009
Ja	61,1 %	74,3 %
Ja, for enkelte av systemene, men ikke alle	16,7 %	I/A
Nei	22,2 %	25,7 %
Antall	18	35

Tabell 6: Er det utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern i den enheten du er resultatenhetsleder for?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
Ja	100,0 %	60,0 %	0,0 %	28,6 %	42,1 %	83,3 %	8,0 %	75,0 %	100,0 %	30,6 %
Nei	0,0 %	40,0 %	100,0 %	57,1 %	47,4 %	16,7 %	88,0 %	25,0 %	0,0 %	66,7 %
Vet ikke	0,0 %	0,0 %	0,0 %	14,3 %	10,5 %	0,0 %	4,0 %	0,0 %	0,0 %	2,8 %
Antall	1	5	1	7	19	6	25	4	1	36

Tabell 7: Har du noen gang lånt ut brukernavn og passord til andre?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
Ja	0,0 %	8,3 %	0,0 %	4,6 %	3,9 %	6,8 %	5,3 %	13,7 %	10,0 %	8,7 %
Ja, men kun til IT-avdeling eller tilsvarende	7,1 %	8,3 %	7,7 %	11,0 %	8,1 %	10,8 %	8,6 %	10,7 %	0,0 %	9,5 %
Nei	92,9 %	83,3 %	92,3 %	83,5 %	86,2 %	81,1 %	84,9 %	74,0 %	80,0 %	80,1 %
Ikke aktuelt	0,0 %	0,0 %	0,0 %	0,9 %	1,8 %	1,4 %	1,3 %	1,5 %	10,0 %	1,6 %
Antall	14	84	13	109	334	74	152	131	10	367

Tabell 8: Hvis jeg skriver ut informasjon som inneholder personopplysninger…

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
Henter jeg alltid utskriften med en gang	42,9 %	29,0 %	8,3 %	32,6 %	28,4 %	94,4 %	86,0 %	87,3 %	100,0 %	88,6 %
Hender det at jeg lar utskriften ligge for å hente den når jeg skal forbi	0,0 %	0,0 %	0,0 %	2,1 %	0,8 %	5,6 %	0,7 %	11,1 %	0,0 %	5,4 %
Ikke relevant, jeg har egen skriver på mitt kontor	0,0 %	5,8 %	0,0 %	14,7 %	9,6 %	0,0 %	11,9 %	1,6 %	0,0 %	5,4 %
Benytter jeg styrt utskrift (også kalt "follow me" eller "sikker utskrift")	50,0 %	63,8 %	91,7 %	45,3 %	54,8 %	I/A	I/A	I/A	I/A	I/A
Ikke aktuelt	7,1 %	1,4 %	0,0 %	5,3 %	6,5 %	0,0 %	1,4 %	0,0 %	0,0 %	0,6 %
Annet	14	69	12	95	261	72	143	126	10	351

Tabell 9: Hva gjør du vanligvis når du i løpet av arbeidsdagen forlater PC-en du bruker?

	2014
Logger ut og/eller slår av datamaskinen	58,6 %
Låser datamaskinen ved hjelp av tastatur eller låseknapp	19,8 %
Baserer meg på at datamaskinen låses automatisk etter noen få minutter	13,2 %
Lukker ned åpne vinduer med informasjon om personopplysninger	5,4 %
Ingenting, tenker ikke så mye på det	2,4 %
Ikke aktuelt	0,6 %
Antall	333

Tabell 10: Har du lest Felles brukerinstruks IKT (tidligere IT-sikkerhetserklæring) for Bergen kommune?

2014	2009

	PPT	Skole	Barne vern	Annet	Total	PPT	Skole	Barne vern	Annet	Total
Ja	57,1 %	63,9 %	61,5 %	64,8 %	67,6 %	70,3 %	88,0 %	83,8 %	70,0 %	82,4 %
Nei	35,7 %	22,9 %	15,4 %	20,0 %	19,6 %	10,8 %	8,0 %	4,6 %	10,0 %	7,4 %
Vet ikke	7,1 %	13,3 %	23,1 %	15,2 %	12,8 %	18,9 %	4,0 %	11,5 %	20,0 %	10,2 %
Antall	14	83	13	105	327	74	150	130	10	364

Tabell 11: I hvilken grad husker du innholdet i Felles brukerinstruks IKT (tidligere IT-sikkerhetserklæring)?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	0,0 %	1,9 %	0,0 %	1,5 %	2,3 %	3,8 %	2,3 %	4,6 %	0,0 %	3,3 %
I stor grad	25,0 %	21,2 %	25,0 %	19,1 %	20,5 %	32,7 %	37,1 %	23,9 %	14,3 %	31,0 %
I noen grad	62,5 %	63,5 %	62,5 %	61,8 %	55,3 %	46,2 %	43,9 %	44,0 %	57,1 %	44,7 %
I liten grad	12,5 %	9,6 %	12,5 %	16,2 %	17,4 %	15,4 %	11,4 %	13,3 %	28,6 %	15,3 %
I svært liten grad	0,0 %	1,9 %	0,0 %	1,5 %	2,7 %	1,9 %	5,3 %	6,4 %	0,0 %	5,0 %
Vet ikke	0,0 %	1,9 %	0,0 %	0,0 %	1,8 %	0,0 %	0,0 %	1,8 %	0,0 %	0,7 %
Antall	8	52	8	68	219	52	132	103	7	300

Tabell 12: I hvilken grad er innholdet i Felles brukerinstruks IKT (tidligere IT-sikkerhetserklæring) forståelig for deg?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	0,0 %	8,9 %	0,0 %	8,9 %	9,4 %	20,9 %	13,6 %	13,9 %	20,0 %	15,2 %
I stor grad	71,4 %	73,3 %	66,7 %	71,4 %	67,6 %	62,8 %	65,5 %	53,2 %	60,0 %	60,8 %
I noen grad	28,6 %	15,6 %	33,3 %	17,9 %	21,8 %	16,3 %	20,0 %	31,6 %	20,0 %	23,2 %
I liten grad	0,0 %	2,2 %	0,0 %	0,0 %	0,6 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
I svært liten grad	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
Vet ikke	0,0 %	0,0 %	0,0 %	1,8 %	0,6 %	0,0 %	0,9 %	1,3 %	0,0 %	0,8 %
Antall	7	45	6	56	170	43	110	79	5	237

Tabell 13: Har du lest Overordnet retningslinje for behandling av personopplysninger i Bergen kommune?

	2014				
	PPT	Skole	Barnevern	Annet	Total
Ja	28,6 %	48,5 %	8,3 %	52,7 %	49,8 %
Nei	42,9 %	31,8 %	41,7 %	23,7 %	25,5 %
Vet ikke	28,6 %	19,7 %	50,0 %	23,7 %	24,7 %
Antall	14	66	12	93	255

Tabell 14: I hvilken grad husker du innholdet i Overordnet retningslinje for behandling av personopplysninger i Bergen kommune?

	2014				
	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	0,0 %	9,4 %	0,0 %	4,3 %	4,8 %
I stor grad	75,0 %	34,4 %	0,0 %	38,3 %	40,0 %
I noen grad	25,0 %	46,9 %	0,0 %	44,7 %	43,2 %
I liten grad	0,0 %	6,3 %	100,0 %	10,6 %	8,8 %
I svært liten grad	0,0 %	0,0 %	0,0 %	2,1 %	0,8 %
Vet ikke	0,0 %	3,1 %	0,0 %	0,0 %	2,4 %
Antall	4	32	1	47	125

Tabell 15: I hvilken grad er innholdet i Overordnet retningslinje for behandling av personopplysninger i Bergen kommune forståelig for deg?

	2014				
	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	0,0 %	13,8 %	0,0 %	15,0 %	11,0 %
I stor grad	75,0 %	62,1 %	0,0 %	70,0 %	67,9 %
I noen grad	25,0 %	24,1 %	0,0 %	15,0 %	20,2 %
I liten grad	0,0 %	0,0 %	0,0 %	0,0 %	0,9 %
I svært liten grad	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
Vet ikke	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
Antall	4	29	0	40	109

Tabell 16: Vet du hvor du finner rutiner og retningslinjer for informasjonssikkerhet på Bergen kommunes intranett?

	2014				
	PPT	Skole	Barnevern	Annet	Total
Ja	71,4 %	69,5 %	53,8 %	72,9 %	73,2 %
Nei	28,6 %	30,5 %	46,2 %	27,1 %	26,8 %
Antall	14	82	13	107	325

Tabell 17: Har du fått tilstrekkelig opplæring i hvordan IT-systemene du benytter skal brukes? Byrådsavdelinger

	2014								
	Barnehage og skole	Byutvikling, klima og miljø	Finans, eiendom og eierskap	Helse og omsorg	Kultur, næring, idrett og kirke	Sosial, bolig og område satsing	Byrådsledersavdeling	Annet	Total
Ja, opplæringen har vært tilstrekkelig	34,5 %	30,0 %	54,8 %	43,4 %	28,6 %	38,7 %	33,3 %	41,7 %	39,8 %
Ja, men ikke i alle IT-systemene jeg bruker	22,4 %	20,0 %	25,8 %	21,7 %	14,3 %	22,6 %	66,7 %	8,3 %	22,3 %

Nei, opplæringen kunne vært bedre	37,9 %	50,0 %	19,4 %	34,9 %	57,1 %	38,7 %	0,0 %	41,7 %	35,8 %
Ikke aktuelt	5,2 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	8,3 %	2,1 %
Antall	116	20	31	106	7	31	6	12	332

Tabell 18: Har du fått tilstrekkelig opplæring i hvordan IT-systemene du benytter skal brukes?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
Ja, opplæringen har vært tilstrekkelig	28,6 %	38,1 %	38,5 %	41,7 %	39,8 %	39,2 %	40,4 %	44,6 %	30,0 %	41,4 %
Ja, men ikke i alle IT-systemene jeg bruker	14,3 %	26,2 %	23,1 %	19,4 %	22,3 %	28,4 %	32,5 %	21,5 %	0,0 %	28,4 %
Nei, opplæringen kunne vært bedre	50,0 %	32,1 %	38,5 %	37,0 %	35,8 %	29,7 %	25,2 %	31,5 %	70,0 %	29,6 %
Ikke aktuelt	7,1 %	3,6 %	0,0 %	1,9 %	2,1 %	2,7 %	2,0 %	2,3 %	0,0 %	2,3 %
Antall	14	84	13	108	332	74	151	130	10	365

Tabell 19: I hvilken grad har din nærmeste ledelse fremhevet viktigheten av informasjonssikkerhet?

	2014					2009				
	PPT	Skole	Barnevern	Annet	Total	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	7,1 %	11,9 %	7,7 %	14,7 %	11,7 %	18,9 %	10,5 %	11,5 %	50,0 %	13,6 %
I stor grad	21,4 %	36,9 %	61,5 %	36,7 %	34,2 %	35,1 %	34,2 %	33,6 %	20,0 %	33,8 %
I noen grad	42,9 %	22,6 %	7,7 %	25,7 %	26,4 %	35,1 %	32,9 %	31,3 %	20,0 %	32,4 %
I liten grad	14,3 %	15,5 %	7,7 %	10,1 %	14,4 %	5,4 %	15,8 %	13,0 %	10,0 %	12,5 %
I svært liten grad	14,3 %	9,5 %	15,4 %	8,3 %	10,2 %	5,4 %	2,6 %	7,6 %	0,0 %	4,9 %
Vet ikke	0,0 %	3,6 %	0,0 %	4,6 %	3,0 %	0,0 %	3,9 %	3,1 %	0,0 %	2,7 %
Antall	14	84	13	109	333	74	152	131	10	367

Tabell 20:I hvilken grad har din nærmeste ledelse fremhevet viktigheten av informasjonssikkerhet? Byrådsavdelinger

	2014								
	Barnehage og skole	Byutvikling, klima og miljø	Finans, eiendom og eierskap	Helse og omsorg	Kultur, næring, idrett og kirke	Sosial, bolig og område satsing	Byrådsledersavdeling	Annet	Total
I svært stor grad	10,3 %	0,0 %	12,9 %	15,0 %	14,3 %	12,9 %	0,0 %	18,2 %	11,7 %
I stor grad	32,8 %	28,6 %	35,5 %	42,1 %	0,0 %	22,6 %	50,0 %	27,3 %	34,2 %
I noen grad	25,9 %	38,1 %	32,3 %	23,4 %	14,3 %	32,3 %	33,3 %	18,2 %	26,4 %
I liten grad	15,5 %	23,8 %	3,2 %	9,3 %	42,9 %	19,4 %	16,7 %	18,2 %	14,4 %
I svært liten grad	11,2 %	9,5 %	12,9 %	7,5 %	28,6 %	12,9 %	0,0 %	9,1 %	10,2 %
Vet ikke	4,3 %	0,0 %	3,2 %	2,8 %	0,0 %	0,0 %	0,0 %	9,1 %	3,0 %
Antall	116	21	31	107	7	31	6	11	333

Tabell 21: I hvilken grad har din nærmeste ledelse fremhevet viktigheten av informasjonssikkerhet? Resultatenhetsledere

	2014	2009
I svært stor grad	5,3 %	2,8 %
I stor grad	15,8 %	27,8 %
I noen grad	21,1 %	39,0 %
I liten grad	36,8 %	22,2 %
I svært liten grad	21,1 %	2,8 %
Vet ikke	0,0 %	5,6 %
Antall	19	36

Vedlegg 2 Høringsuttale

Vedlagt er høringsuttale fra Byrådsavdeling for finans, eiendom og eierskap.

BERGEN KOMMUNE

BYRÅDSAVDELING FOR FINANS, EIENDOM OG EIERSKAP
Bergen Rådhus
Postboks 7700, 5020 Bergen
Sentralbord 05556
Telefaks 55 56 69 15
finans@bergen.kommune.no
www.bergen.kommune.no

Deloitte

Deres ref.	Deres brev av:	Vår ref.	Emnekode	Dato
		201300274-51 INKV	ESARK-126	10. april 2015

Høringsuttalelse til forvaltningsrevisjonsrapport om informasjonssikkerhet i Bergen kommune.

1. Innledning

Byrådsavdeling for finans, eiendom og eierskap (BFEE) har mottatt høringsutkast til prosjektrapport fra forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune. I rapporten vurderer Deloitte kommunes oppfølging av tidligere forvaltningsrevisjon av informasjonssikkerhet og behandling av personopplysninger i Bergen kommune (2009). Kommunaldirektør for finans og eierskap gir med dette sin høringsuttalelse til Deloittes rapport.

Kommunaldirektøren er positiv til at det er gjennomført en ny forvaltningsrevisjon av informasjonssikkerhet i Bergen kommune. Tidspunktet for revisjonen er ideelt med tanke på at BFEE for tiden utarbeider forslag til ny informasjonssikkerhetsstrategi for kommunen. BFEE vil vurdere alle funn i Deloittes forvaltningsrevisjonsrapport i tilknytning til dette arbeidet. På generelt grunnlag ser vi hvordan forvaltningsrevisjoner på en rekke områder bidrar positivt til kommunens arbeid med kontinuerlig forbedring.

I denne høringsuttalelsen ønsker kommunaldirektøren å kommentere noen hovedlinjer i arbeidet med informasjonssikkerhet i Bergen kommune. Kommunaldirektøren ønsker blant annet å vise hvordan arbeidet med informasjonssikkerhet vil nyte godt av et generelt skjerpet søkelys på arbeidet med å sikre betryggende kontroll på de gjennomgående konsernområdene som BFEE har ansvar for. Avslutningsvis gis noen konkrete kommentarer til Deloittes anbefalinger.

2. Informasjonssikkerhetsarbeidet i Bergen kommune

Strategi for informasjonssikkerhet, samhandling og styringssystem
Bergen kommune utarbeidet for første gang en strategi for informasjonssikkerhet for perioden 2011 – 2014. Strategien ble behandlet i bystyret 28.03.11 (sak 64-11). Pt er en ny informasjonssikkerhetsstrategi under utarbeidelse. I arbeidet med den nye strategien tas det utgangspunkt i erfaringene med den gamle, herunder grunnene til at flere av tiltakene i

strategien ikke er realisert. Blant annet vil den nye strategien legge opp til at det skal jobbes mer systematisk med tverrfaglig integrasjon innen internkontroll og sikkerhetsarbeid for øvrig. En ønsker med det å få en tydeligere oppmerksomhet på informasjonssikkerhet som del av det generelle arbeidet for å sikre betryggende kontroll i og med virksomheten. Som for den forrige strategien legges det til grunn en forståelse av at informasjonssikkerhet handler om sikring av informasjon, uavhengig av om behandlingsmåten er elektronisk eller manuell.

Et viktig budskap i arbeidet med å skape et godt sikkerhetsmiljø i Bergen kommune er at mennesker utgjør den vesentligste risikoen. Det er i mange tilfeller ansattes handlinger – eller mangel på handlinger - som medfører risiko for at informasjon skal komme på avveier. Fra overordnet nivå i organisasjonen legges det vekt på å utvikle informasjons-, veilednings- og opplæringsopplegg, som skaper bevissthet omkring dette blant kommunale ledere og ansatte. Direktør for IKT Konsern har som del av sine fagfullmakter fått videredelegert kommunaldirektørens myndighet til å følge opp og etterse at det i hele kommunens organisasjon etableres et opplegg for informasjonssikkerhet som sikrer god egenkontroll i oppgaveløsningen i de enkelte enheter, i samsvar med eForvaltningsforskriften, Nasjonal strategi for informasjonssikkerhet og særlovgivning som personopplysningsloven og helseregisterloven. Avdeling for informasjonssikkerhet i IKT Konsern skal prioritere samhandling med de øvrige byrådsavdelingene for å sikre dette. Innad i BFEE er det dannet fagnettverk i regi av den nyopprettete seksjonen for internkontroll, som skal skape synergier i arbeidet med å utvikle internkontrollfunksjonen på de gjennomgående konsernområdene BFEE har ansvar for (økonomisk internkontroll, HR, HMS, anskaffelser, informasjonssikkerhet).

I en virksomhet med mer enn 400 IKT-systemer i bruk, er samtidig teknologidimensjonen svært sentral i informasjonssikkerhetsarbeidet. Det må således legges vekt på god samhandling innenfor IKT-området i henhold til vedtatte fullmakter og gjeldende avtaler. Direktør for IKT Konsern har fagfullmakt som overordnet myndighet for sikkerhet i kommunens IKT-systemer. I utgangspunktet er all fagmyndighet lagt til IKT Konsern som bestiller. Fagmyndighet lagt til IKT Drift skal fremgå av oppdragsavtalen som ligger til grunn for bestiller-/utførermodellen på oppgaveområdet. Den nye informasjonssikkerhetsstrategien skal i større grad enn tidligere følges opp gjennom bestiller-leverandør-modellen på IKT-området og i driftstjenesteavtalen mellom IKT-konsern og IKT Drift. I tillegg skal disse enhetene, som alle andre enheter i kommunen, følge kommunens vedtatte styringssystemer på ulike konsernområder, herunder informasjonssikkerhet.

I henhold til eForvaltningsforskriften er kommunen pålagt å 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 (eForvaltningsforskriftens § 15 andre ledd). Revisor vurderer at dagens overordnete styringssystem for informasjonssikkerhet i Bergen kommune har noen vesentlige mangler ut fra de rutinene og retningslinjene som er gjeldende i dag. Kommunaldirektøren for finans og eiendom tar revisors påpekning til etterretning og vil fremover prioritere arbeidet med å konsolidere et fullverdig, felles styringssystem for informasjonssikkerhet i Bergen kommune. Styringssystemet skal knyttes til den ordinære styringsstrukturen og vil fremstå som et «styrings- og internkontrollsystem for informasjonssikkerhet» basert både på ISO/IEC 27001:2013 og generelt på god praksis. Det kan i denne sammenheng nevnes at det er etablert dialog og samarbeid med nasjonale aktører som NorSIS, DIFI og Datatilsynet.

3. Kommentarer til Deloittes anbefalinger

Med bakgrunn i funnene i den gjennomførte forvaltningsrevisjonen anbefaler Deloitte at Bergen kommune vurderer å gjennomføre følgende tiltak:

1. Utbedre de elementene i styringssystemet hvor det er påpekt mangler, med særlig vekt på
    a) Risikovurderinger
    b) Sikkerhetsrevisjoner
    c) Avvikshåndtering
    d) Ledelsens gjennomgang

2. Sørge for at systemeiere har tilstrekkelig opplæring og støtteverktøyer for å kunne gjennomføre sine oppgaver.

3. Sørge for at retningslinjer og rutiner på informasjonssikkerhet er oppdatert og sikrer at alle ansatte kjenner til hvor man finner rutinene.

4. Ved utarbeidelse av ny strategi for informasjonssikkerhet, fastsette krav til oppfølging av og rapportering på gjennomføring av tiltak, samt eventuell rullering av planer og tiltak.

Kommunaldirektør for finans og eierskap gir følgende kommentarer til anbefalingene fra Deloitte:

1. Utbedre elementer i styringssystemet hvor mangler er påpekt

a. Risikovurderinger

Det er, siden forrige revisjon av informasjonssikkerhet i 2009, innarbeidet konkrete krav til risikovurderinger og informasjonssikkerhet i både prosjekt- og forvaltningsprosesser innen IKT-området. Risiko skal nå være en integrert del av arbeidet med kravspesifisering, prosjekt og systemforvaltning. Bevisstgjøring og implementering er en del av det kontinuerlige forbedringsarbeidet.

Våren 2014 ble det gjennomført et risikostyringsprosjekt i regi av BFEE, hvor samtlige byrådsavdelinger deltok. Gjennom prosjektet ble det tilrettelagt en metode og et verktøy for risikovurderinger generelt, som skal gjennomføres i alle deler av kommunens virksomhet. Fra 2015 skal alle byrådsavdelingene gjennomføre overordnede risikovurderinger av egne ansvars- og myndighetsområder, som grunnlag for grundigere analyser på fagområder som utmerker seg med høy risiko. Vurdering av risiko for informasjonssikkerhet skal være en del av dette arbeidet.

b. Sikkerhetsrevisjoner

Avdeling for informasjonssikkerhet i IKT Konsern er i ferd med å utarbeide plan og rutiner for sikkerhetsrevisjoner. Avdelingen er bemannet opp med ett årsverk som for tiden har dette som sin primære oppgave.

c. Avvikshåndtering

Det er en prioritert oppgave å gjøre systemet som er etablert for registrering og rapportering av avvik på informasjonssikkerhetsområdet bedre kjent i organisasjonen. Registrering av

informasjonssikkerhetsavvik er blant de tema som er tatt med i kommunens internkontrollundersøkelse overfor ledere (fra 2015). I forbindelse med operasjonalisering av byrådssak 1401/14 *Internkontroll i Bergen kommune. Overordnet rammeverk,* vil det settes et generelt forsterket søkelys på registrering og oppfølging av avvik i hele kommunens organisasjon.

d. Ledelsens gjennomgang

I tilknytning til arbeidet med ny strategi for informasjonssikkerhet vurderes det hvordan ledelsens gjennomgang skal organiseres. Revisors anbefaling om at jevnlig (årlig) ledelsesgjennomgang av sikkerhetsmål og strategi bør fastsettes i en rutine, for å sikre oppfyllelse av personopplysningsforskriften § 2-4, tas med i disse vurderingene.

2. *Systemeiere*

IKT Konsern utarbeider nå et nytt styrende dokument, hvor blant annet systemeierrollen defineres mer presist hva gjelder ansvar og oppgaver. Det skal legges større vekt på opplæring.

3. *Retningslinjer og rutiner for informasjonssikkerhet*

Ny håndbok for informasjonssikkerhet er under utvikling og skal etter planen gjøres tilgjengelig ved innføring av ny intranettløsning som pågår. Det vil bli iverksatt et arbeid knyttet til å formidle innhold og sikre forståelse av innholdet i den nye håndboken.

Kjennskap til kommunens retningslinjer for informasjonssikkerhet er blant spørsmålene i kommunens internkontrollundersøkelse overfor ledere fra 2015. Det stilles spørsmål om leder kjenner til de interne retningslinjene i kommunen, og om retningslinjene er gjort kjent for ansatte i resultatenheten. Når svarene foreligger, vil nødvendige aktiviteter for å bedre kjennskapen til retningslinjene iverksettes i samarbeid med byrådsavdelingene.

Slik det går frem av overordnet rammeverk for internkontroll i Bergen kommune (byrådssak 1401/14) ligger det til BFEEs konsernrolle et ansvar for å utvikle og holde ved like felles, overordnede rutiner og systemer, samt myndighet til å etterse at felles overordnede rutiner og systemer implementeres i hele kommunens virksomhet på en tilfredsstillende måte. For å sikre en praksis i henhold til regelverket vil det i løpet av 2015 legges planer for systematiske etterkontroller på informasjonssikkerhetsområdet.

4. *Fastsette krav til oppfølging og rapportering på gjennomføring av tiltak, og eventuell rullering av planer og tiltak*

Revisors anbefaling følges opp i arbeidet med ny informasjonssikkerhetsstrategi.

Med hilsen

Ingvild Kvilekval - saksbehandler
Ove Foldnes - kommunaldirektør

Dette dokumentet er godkjent elektronisk.

Vedlegg 3: Oversikt over sentrale dokument og litteratur

Regelverk

Forskrift om behandling av personopplysninger (personopplysningsforskriften). FOR-2000-12-15-1265.

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

Lov om behandling av personopplysninger (personopplysningsloven). LOV-2000-04-14-31

Veiledere og standarder

BS ISO/IEC 27001 :2013 «Information technology - Security techniques - Information security management systems – Requirements»

BS ISO/IEC 27002:2013 «Information technology - Security techniques – Code of practice for information security controls»

Datatilsynet: En veiledning om internkontroll og informasjonssikkerhet. 2009.

Datatilsynet: Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer. Desember 2000. SV-100:2000.

Difi: referansekatalogen. http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon/#Styringssystem

Helsedirektoratet: Norm for informasjonssikkerhet. Helse og omsorgstjenester. 2015.

Koordineringsutvalg for informasjonssikkerhet (KIS): "Klassifisering Og Beskyttelse av Informasjon", 2008.

Kommunale vedtak og dokument

Bergen kommune: Bergen kommunes strategi for informasjonssikkerhet (2011 – 2014).

Bergen kommune: IKT Drift – avklaring vedrørende organisasjonsmodell. Byrådssak 1058/14.

Bergen kommune: Årsoppdrag 2014 – IKT Konsern (saksnr. 201406071-3)

Bergen kommune, kommunerevisjonen: Forvaltningsrevisjonsprosjektet Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune. Revisjonsrapport 69 (2009).