NORDISK SAMARBEJDE OM INFORMATIONSSIKKERHED I KOMMUNER OG REGIONER

NOTAT OM INFORMATIONSSIKKERHED OG DIGITALISERING

DANSKE KOMMUNER 2014

2008 – 2014

Notatet er udarbejdet for:

Oktober 2014

INDLEDNING

Digitaliseringen i form af selvbetjeningsløsninger for borgere og virksomheder, nye mulighed for virtuel kommunikation med omverdenen, mobile og fleksible arbejdspladser og anvendelsen af sociale medier i arbejdsmæssig og privat sammenhæng, betyder en flytning af behandlingen af data fra få store systemer og manuelle processer, til nye digitale platforme.

Risikobilledet for den kommunale informationsanvendelse fremstår på flere områder mere omfattende og komplekst nu end før:

- Pålideligheden og troværdigheden af data kontrolleres oftere i systemer end af mennesker
- Tilgængelighed af systemer og data er i fokus, hvor adgangen til information sker gennem systemer
- Data kan befinde sig på mange forskellige IT-platforme i kommunen, der ofte kun delvist er i kommunens kontrol

Informationssikkerhed er et område, der er stor opmærksomhed på i offentligheden:

- En kommende EU-forordning skærper kravene til behandlingen af personfølsomme data og fastlægger bl.a. krav til ansvarsforhold på niveau med det som kendes i Norge og Sverige
- En række hændelser har vist sårbarheden i IT-systemerne for kriminelle handlinger og interne fejl og misbrug.

Indtil for et par år siden kunne kommunerne orientere sig efter en fælles dansk rammestandard, DS 484, der fastlagde minimumsindsatser for informationssikkerhed. Standarden er i statslige organisationer afløst af ISO 27001, der tager udgangspunkt i en tættere sammenhæng mellem forretningsorganisationen og det nødvendige niveau for informationssikkerhed, men uden at foreskrive konkrete minimums indsatser. KL anbefaler at kommunerne anvender ISO-standarden med henblik på at få en fælles, høj sikkerhedsstandard i den offentlige sektor. Det stiller en række forventninger til organisationens evne og kompetence til at arbejde med informationssikkerhed:

- Den øverste ledelses ansvar for mål for og opfølgning på organisationens informationssikkerhed
- Forretningsorganisationens ansvar for at tilrettelægge en sikker brug af IT.

I notatet vises, hvor langt de danske kommuner er kommet på disse områder og hvordan rammerne for informationssikkerhed er tilrettelagt.

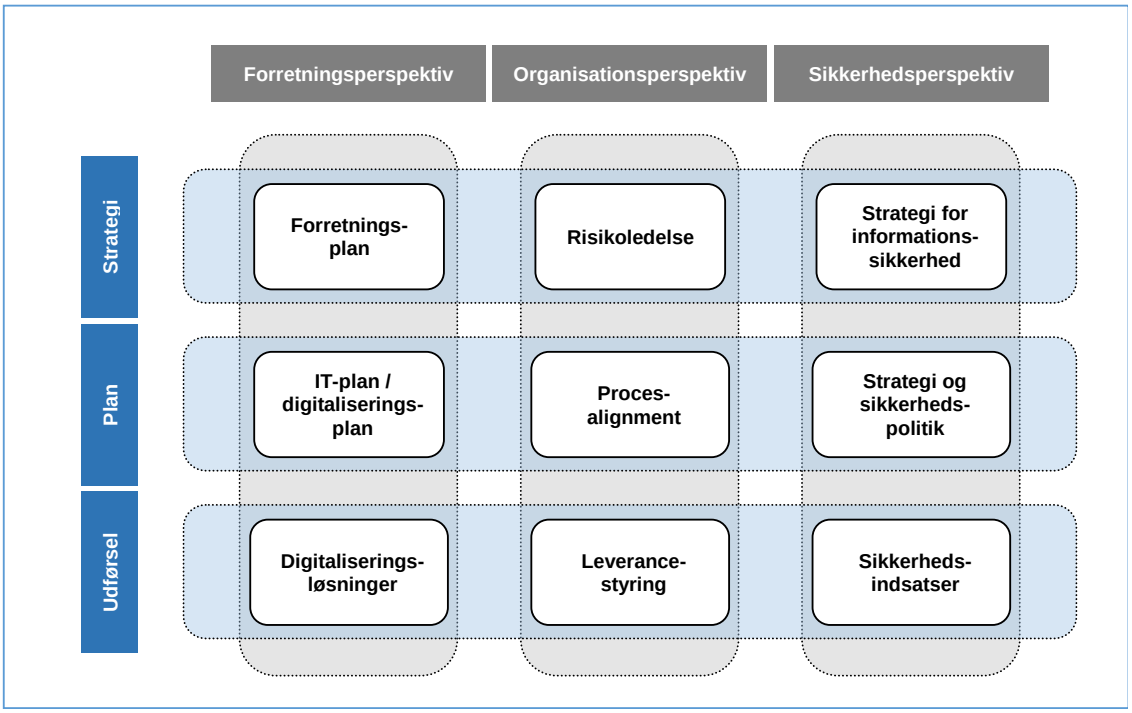
Notatet er udformet med afsæt i den nordiske undersøgelse af informationssikkerhed i kommuner og regioner. Hver fjerde kommune i Danmark har svaret på alle spørgsmål i undersøgelsen svarende til 37 % af indbyggertallet. I 2012 var det 35%.

Af de deltagende kommuner har 75% medvirket i begge undersøgelser. De syv kommuner, der er nye i 2014, tæller med sammen med øvrige, hvilket kan give forrykninger i de summerede opgørelser for 2014.

Undersøgelsens spørgetema er tilrettelagt således den afspejler organisationens samlede fokus på informationssikkerhed – fra den øverste ledelse, til det konkrete arbejde. Endvidere har spørgetemaet fokus på kommunernes anvendelse af IT og de risikovurderinger, der gøres. Undersøgelsen fastholder spørgsmål, der viser tilbage til 2012 og tidligere, men søger samtidig at afdække tendenser i IT-anvendelsen og initiativer til sikring.

Endelig har undersøgelsen en række spørgsmål om oplevede hændelser og følgerne af disse.

Sammenhængen mellem den forretningsmæssige anvendelse af systemer og informationer ift. kommunernes overvejelser om informationssikkerhed er udtrykt i nedenstående model:



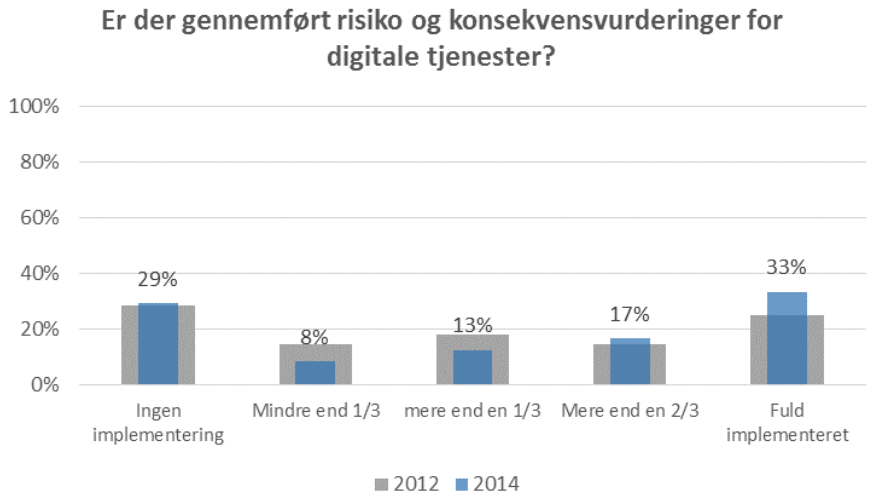
For indblik i undersøgelsens øvrige talmateriale henvises til det benchmark-materiale som kommunerne kan erhverve ved henvendelse til I-Trust.

INFORMATIONSSIKKERHED OG DIGITALISERING

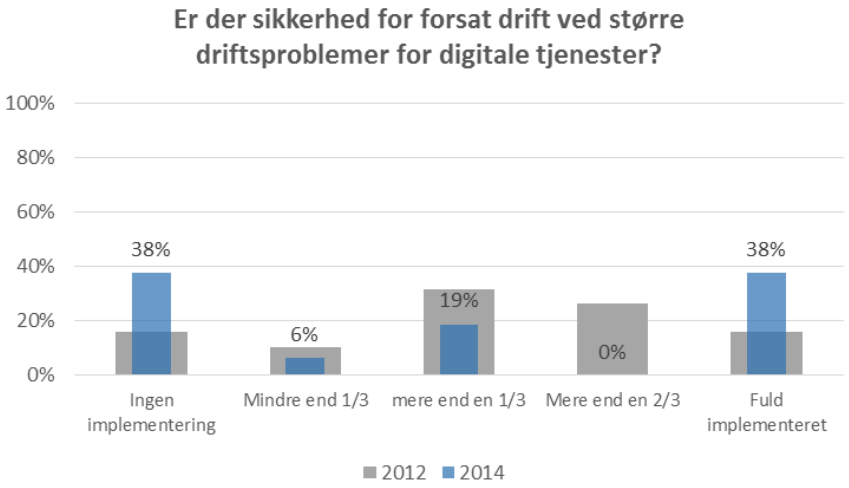
Digitalisering

I forbindelse med omlægning af borgerservices fra medarbejder-betjente processer til digitaliserede og automatiserede tjenester, der tilgås via internettet, ændres risiko-billedet på flere områder – truslerne mod såvel tjenesternes tilgængelighed og informationernes fortrolighed, som konsekvenserne af brud skifter karakter, hvis der sker fejl og andre brud.

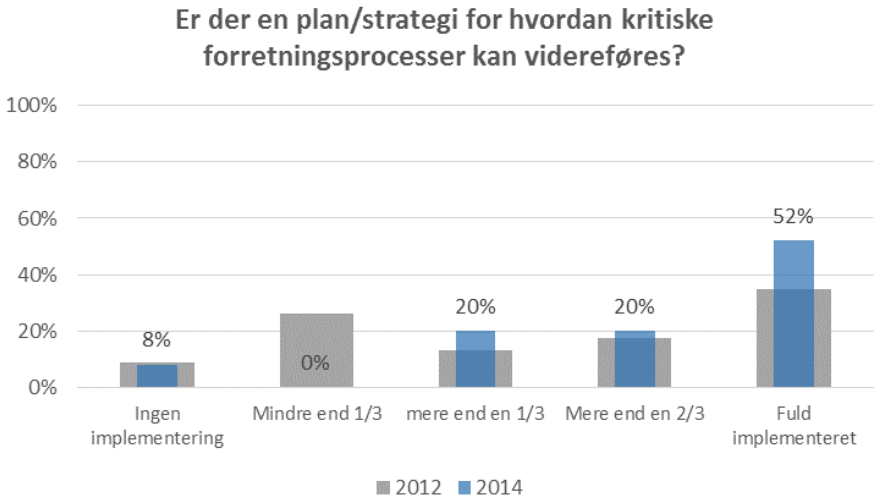
Fra 2012 til 2014 gennemfører flere kommuner risiko og konsekvensvurderinger, og tælles kommuner med, der er langt i processen, er det hver anden kommune, der har fokus på dette område.



Med omlægningen til digitale tjenester er kravet ikke udelukkende tilgængelighed af medarbejdere og systemer, men også borgere og virksomheders tilgang til digitale tjenester.
Den øgede fokus på risikostyringen afspejler sig i, at fire ud af ti kommuner har sikret, at driften kan foresætte i tilfælde af IT-problemer. Det ses også, at en større del af kommunerne ikke har truffet disse forholdsregler:



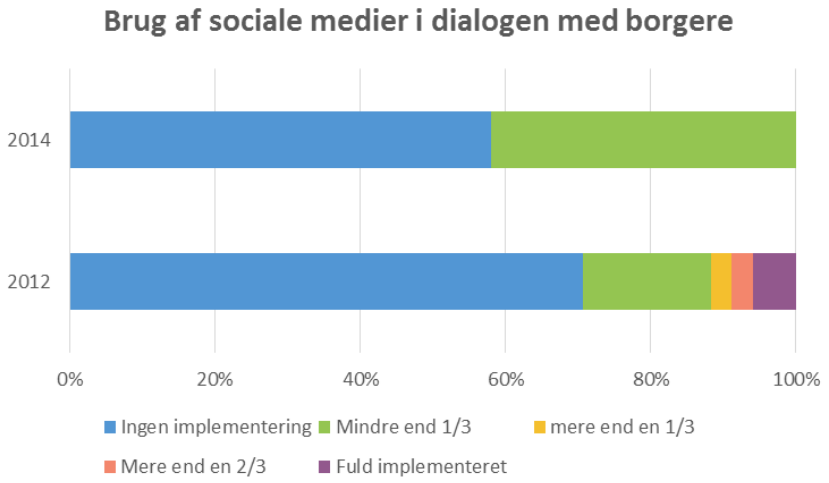
Kommunerne er i stigende omfang opmærksomme på, at kritiske processer skal kunne videreføres, hvis der er problemer til med tilgang til IT eller andre kritiske ressourcer. Mere end hver anden kommune har en Business Continuity Plan, dvs. en plan for hvordan services kan udføres, hvis kritiske ressourcer ikke er tilgængelige:



En fungerende Business Continuity Plan forudsætter, at der er lokale indsatsplaner i de enkelte forretningsområder: syv ud af ti kommuner har dette helt eller delvist på plads mod fem ud af ti i 2012. Hver tredje kommune har en plan for regelmæssig uddannelse i og aftestning af beredskabet.

Digital dialog

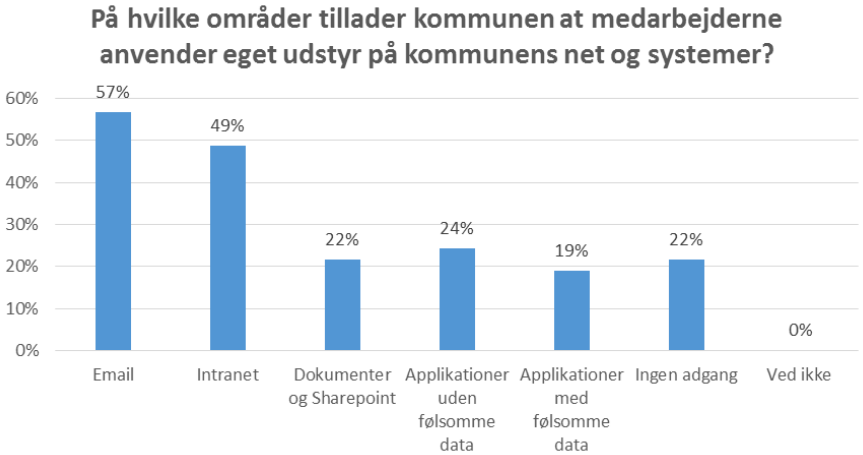
I 2012 var der en begyndende tendens til at kommunerne udnyttede informations-teknologien til digital dialog med borgerne. Tendensen er forsat i 2014, hvor hver fjerde kommune arbejder med dette. Den digitale dialog omfatter brug af de sociale netværks muligheder for chatfunktioner, information via facebook m.v.



Hver fjerde kommune arbejder i et vist omfang med brug af audio/video-faciliteter som eksempelvis Skype som platform for dialog med borgere og virksomheder: tallet er uforandret fra 2012.

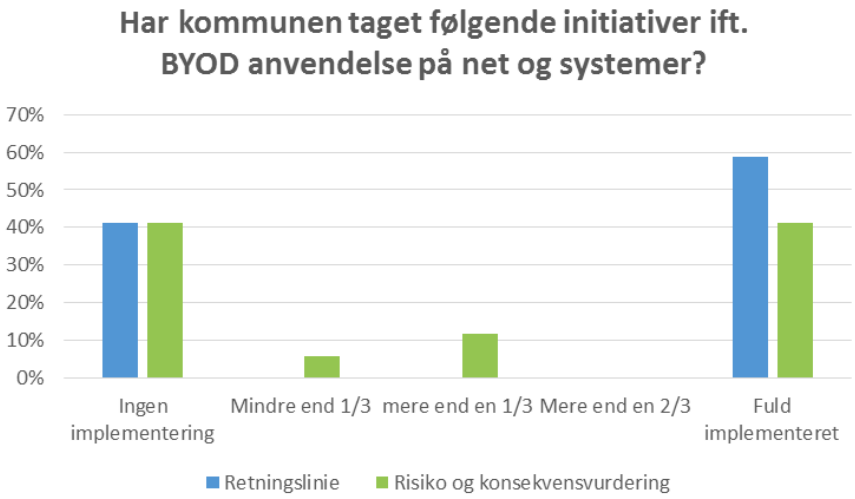
Ny teknologi

De senere år er der sket en betydelig spredning af det udstyr, der anvendes i forbindelse med informationssystemerne (mobile arbejdspladser, telefoner etc.). Denne tendens forstærkes af, at medarbejderne i stigende omfang efterspørger muligheden for at anvende eget udstyr på organisationernes net – både i privat regi, men også opgavemæssigt. I undersøgelsen i 2012 svarede over halvdelen af kommunerne at de tillod medarbejderne at bruge eget udstyr: det samme billede ses i 2014.



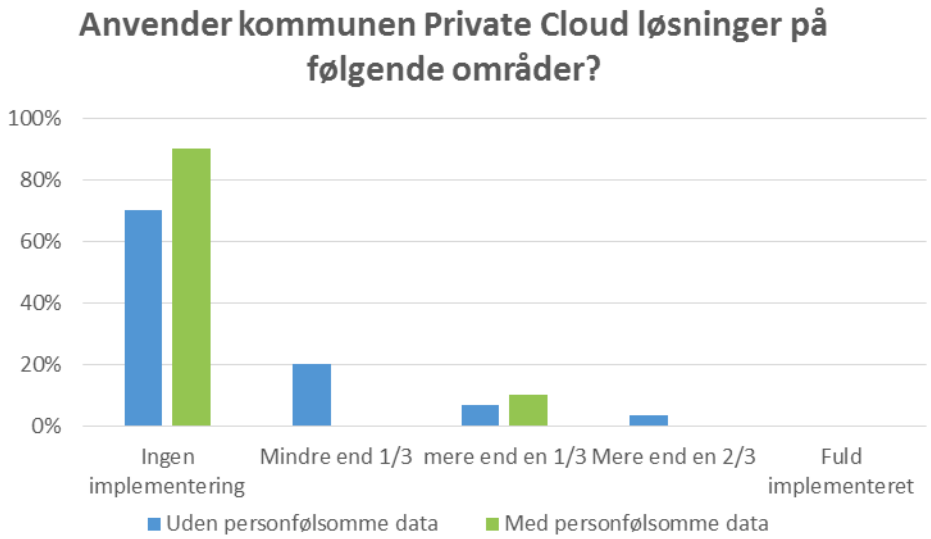
Seks ud ti kommunerne tillader, at medarbejderne kan bruge eget udstyr til kommunens email system og hver femte giver adgang til applikationer med følsomme data.

Blandt de, der tillader medarbejdernes brug af eget udstyr på egne net og systemer, har seks ud ti gennemført risiko- og konsekvensvurdering og fire ud af ti har retningslinier på området:

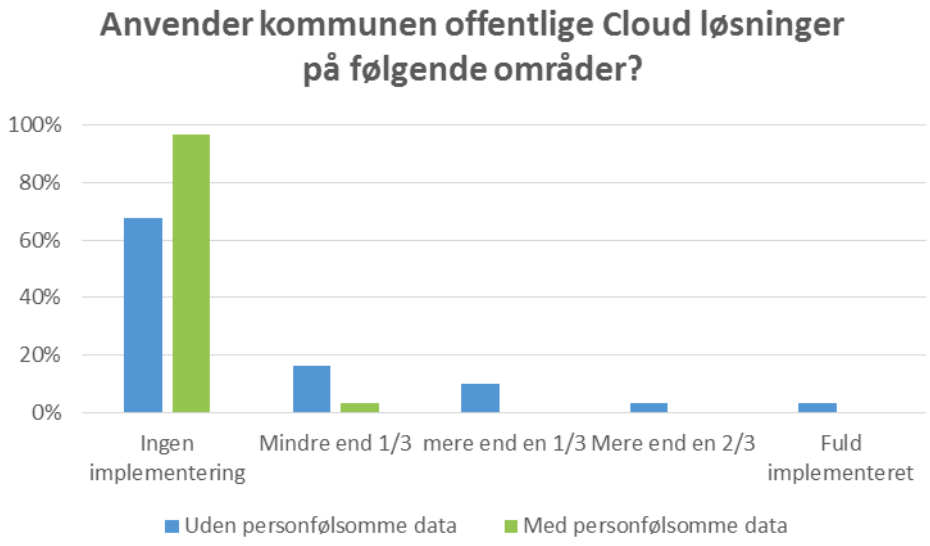


Brug af Cloud-tjenester

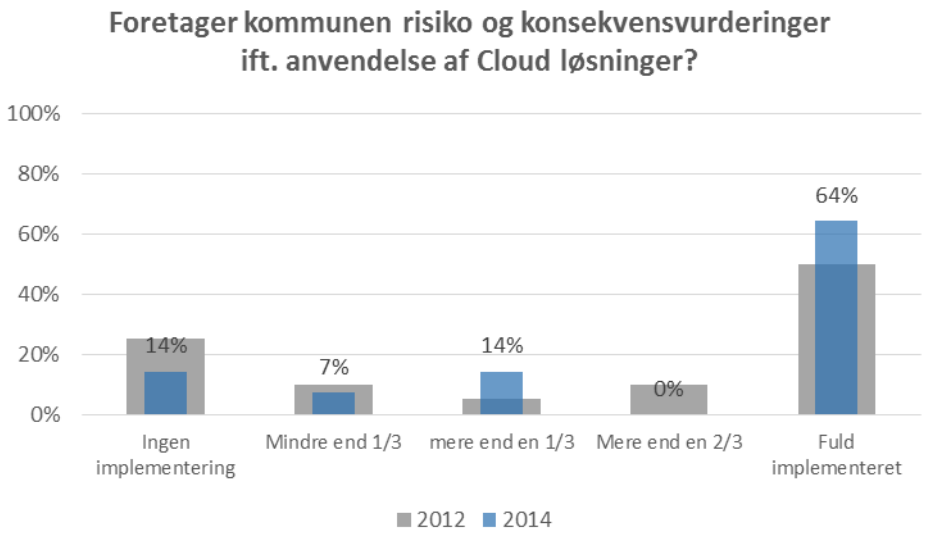
Anvendelsen af Cloud-tjenester på områder, der indeholder personoplysninger, har været drøftet længe i Danmark. Som det fremgår, er det få kommuner, der bruger dedikerede (private) Cloud-tjenester på områder og en meget begrænset anvendelse, hvis der er personoplysninger:



For brugen af offentlige cloud løsninger ses, at kommunerne i et vist omfang bruger det til ikke personfølsomme data:



Der er en række anbefalinger for styring af sikkerhed i forbindelse med anvendelse af Cloud-løsninger; afgørende er, at organisationen tager stilling til de risici, der knytter sig til de Cloud-baserede ydelser:

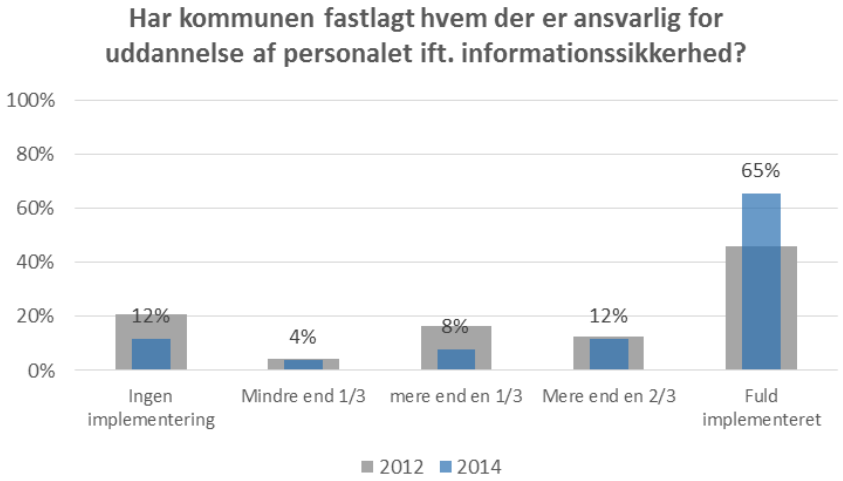


Udviklingen fra 2012 viser, at Cloud anvendelsen i stigende omfang skal ses ud fra en risikovurdering.

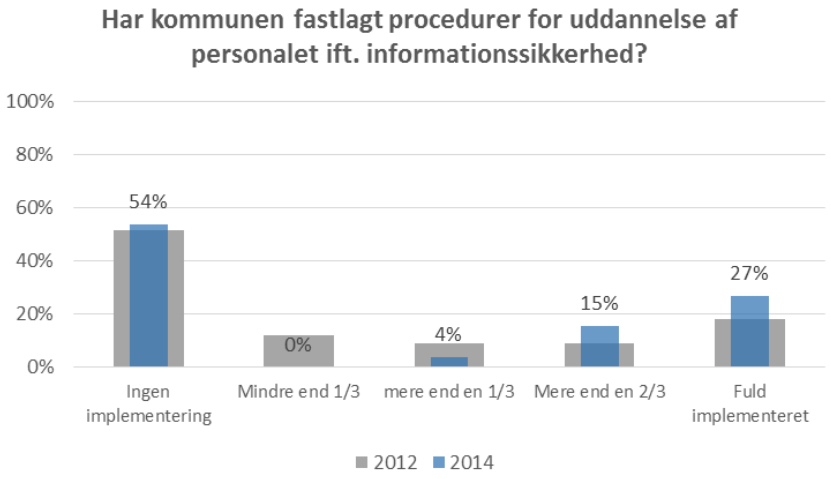
Kompetencekrav til organisationen

Med brugen af digitale tjenester og digitale platforme – mail, digital dialog m.v. – konfronteres medarbejderen med andre og anderledes udfordringer end før.

Det fremgår, at to ud af tre kommuner har fastlagt et formelt ansvar i organisationen for at medarbejderne har tilstrækkelige og relevante kompetencer for sikker anvendelse:



Hver fjerde kommune har fastlagt rammerne for gennemførelse af uddannelse af medarbejdere – en stigning ift. 2012, hvor det var hver femte. Halvdelen af kommunerne – samme andel som i 2014 – arbejder ikke med dette område:

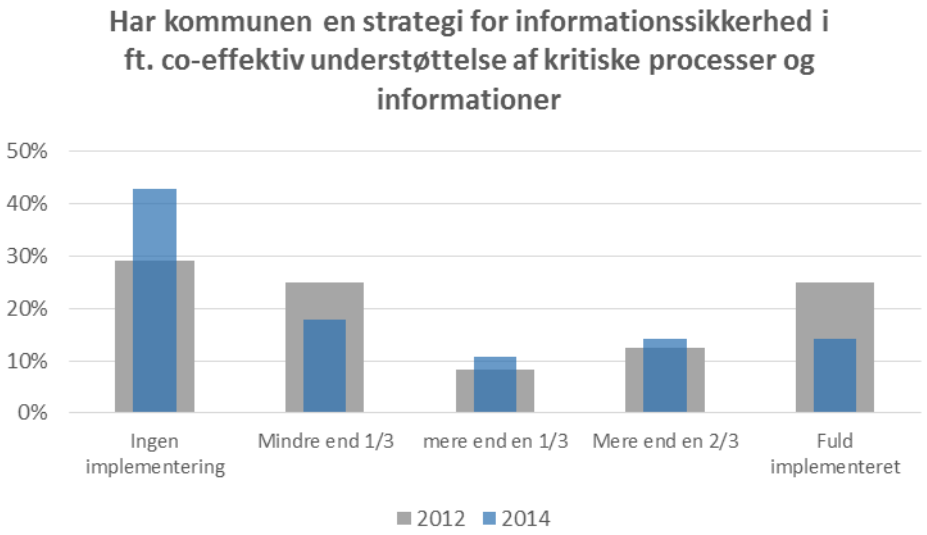


Hver fjerde kommune har afsat midler til at arbejde med uddannelse – i 2012 var det hver femte.

Undersøgelsen i 2012 viste, at ingen af de deltagende kommuner gennemførte målinger af, hvorvidt medarbejderne har tilstrækkelige kompetencer til sikker anvendelse af systemer og informationer. I 2014 er dette forhold ændret således hver femte kommune helt eller delvist har indført sådanne vurderinger. Hver anden af disse kommuner rapporter resultatet af målingerne til den øverste ledelse.

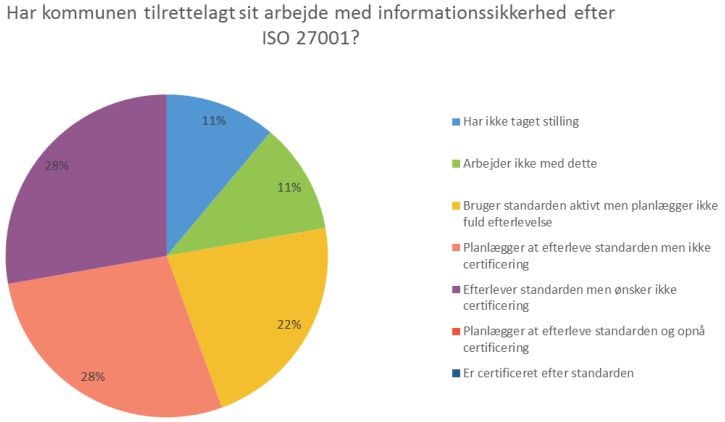
Informationssikkerhed i organisationen

Indførelsen af digitale tjenester og brug af den digitale platform foregår i tæt samarbejde med forretningsområderne i kommunerne. Ændringsprocesserne og den fremadrettede styring vedrører således i høj grad forretningsområdernes opgaver og ansvar.



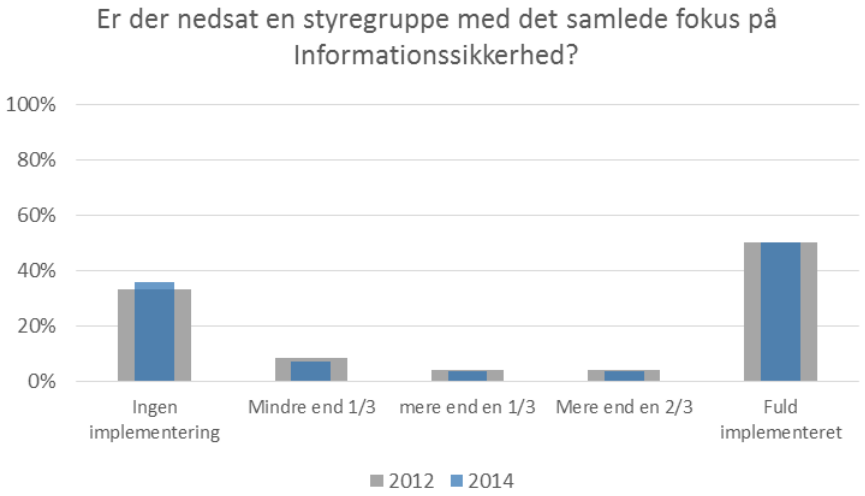
Hver fjerde af kommunerne arbejder med en egentlig forretningsstrategi for informationssikkerhed – færre end i 2012.

Tallet skal ses i forhold til hvor mange af kommunerne, der har tilrettelagt deres arbejde efter en generel norm for informationssikkerhed. Resultatet viser, at ingen af de deltagende kommuner er eller planlægger at blive certificeret i forhold til ISO 27001. Derimod efterlever hver fjerde kommune standarden, en fjerdedel planlægger efterlevelse og hver femte kommune tilrettelægger arbejdet efter denne.



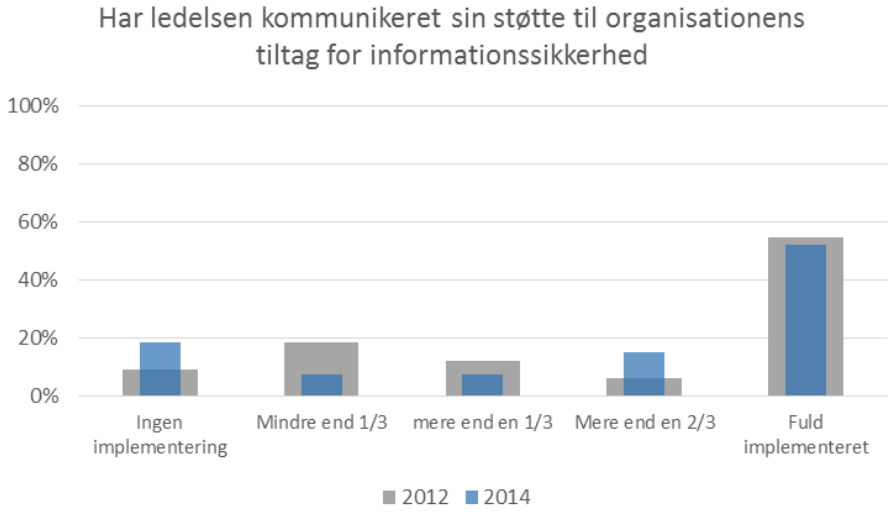
Orienteringen mod ISO 27001 viser at kommunerne – uanset at der ikke er en forretningsstrategi – har tilrettelagt arbejdet med informationssikkerhed ift. en fast ramme.

Forankringen af arbejdet med informationssikkerhed i organisationen omfatter hos halvdelen af kommunerne etablering af styregrupper med samlet fokus på området – det er samme andel som i 2012.

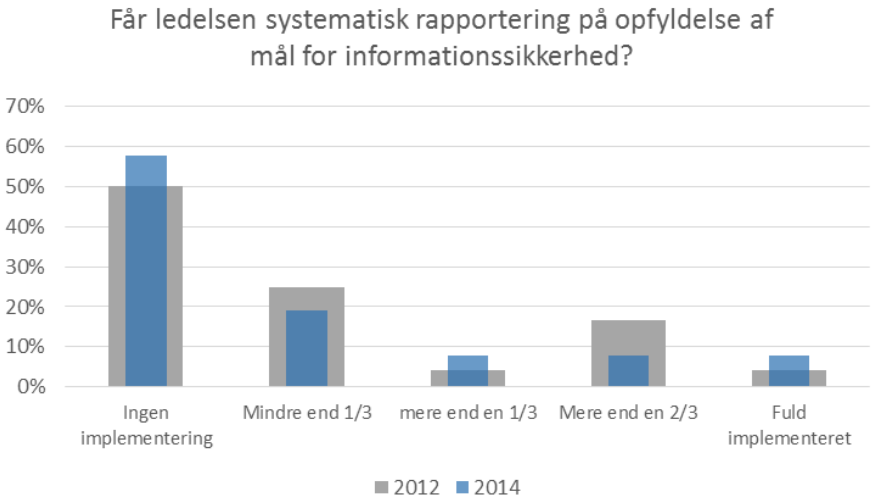


Informationssikkerhed som ledelsesområde.

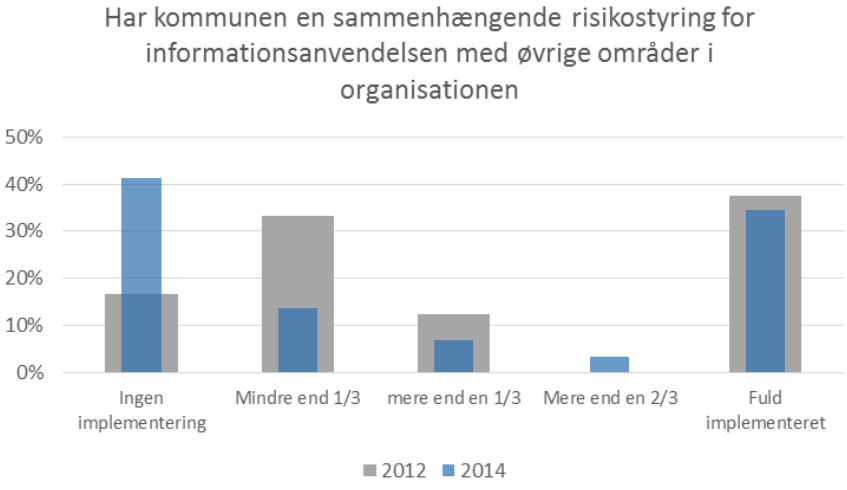
Ledelsens synlige støtte til organisationens arbejde med informationssikkerhed fremhæves ofte som en afgørende faktor for god praksis. Det er tilfældet i seks ud af ti kommuner – samme andel som i 2012:



Der ses en væsentlig forskel på, hvorvidt ledelsens støtte til arbejdet med informationssikkerhed følges op af en regelmæssig og systematisk rapportering af status til ledelsen. Under 10% af kommunerne arbejder med dette:



Et af de områder, hvor ledelsen kan udøve indflydelse på sikkerhedsarbejdet er gennem grundlaget for risikostyring – ved sikring af, at der anvendes metoder, der er kendte og ligner organisationens øvrige risikostyring, samt at der ensartet tages stilling til de identificerede risici.



Mindre end halvdelen af kommunerne har fastlagt en risikovurdering for IT anvendelsen, der er sammenhængende med organisationens øvrige risikostyring og ni ud af ti kommuner har ikke udarbejdet kriterier for hvad der er acceptable risici.

For de kommuner, der ikke har en samlet fokus på risici, kan risikostyringen af IT-anvendelsen blive en styrings-ø i forhold til den øvrige risikostyring i organisationen.