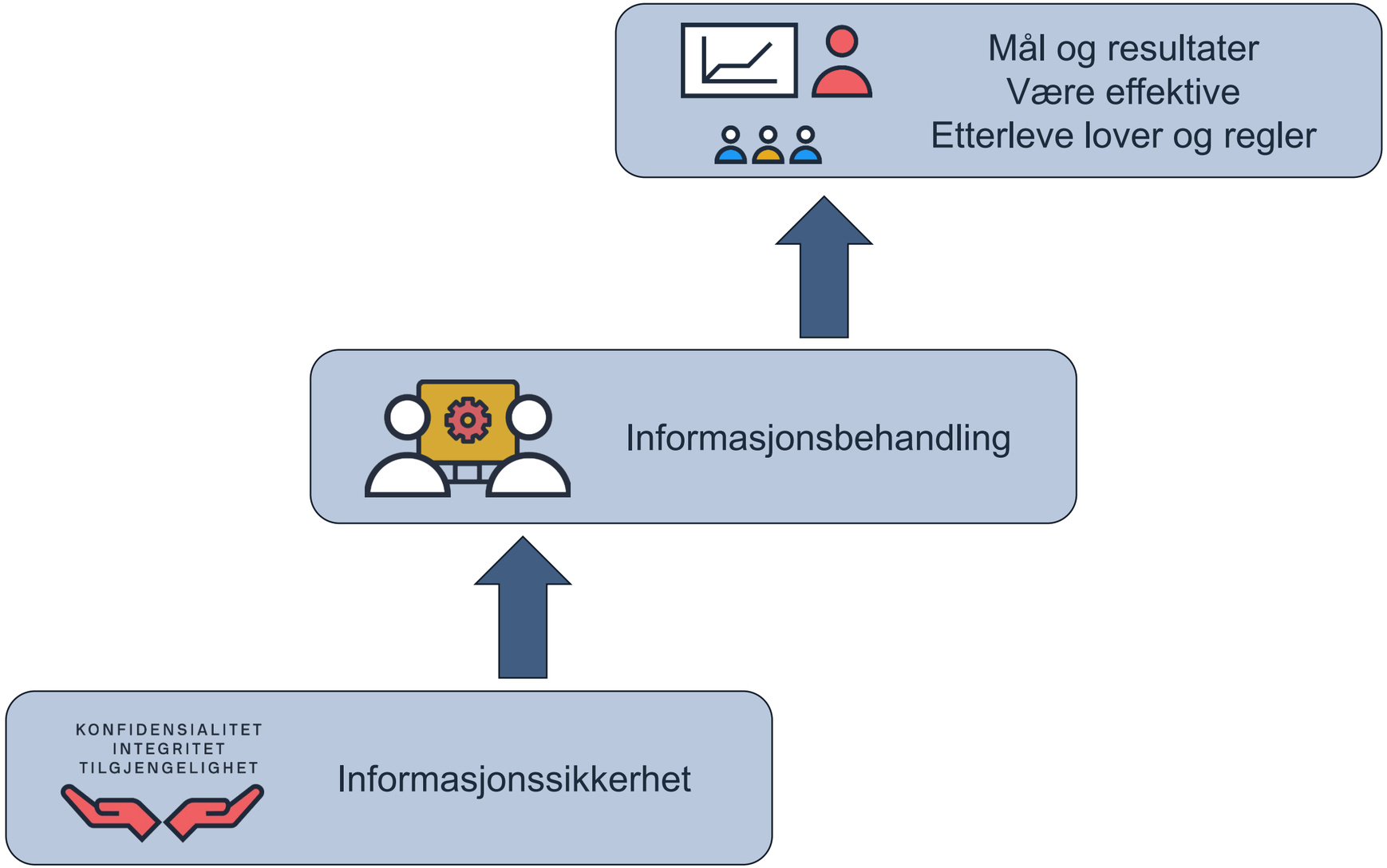
Digdir

digdir.no

Sikkerhetskultur

Katrine Aam Svendsen
Seksjon for informasjonssikkerhet
NIFS – 17.02.2021


Mål og resultater
Være effektive
Etterleve lover og regler
Informasjonsbehandling
KONFIDENSIALITET
INTEGRITET
TILGJENGELIGHET
Informasjonssikkerhet

Internkontroll for informasjonssikkerhet

Ledelsens styring og oppfølging

Risikovurdering

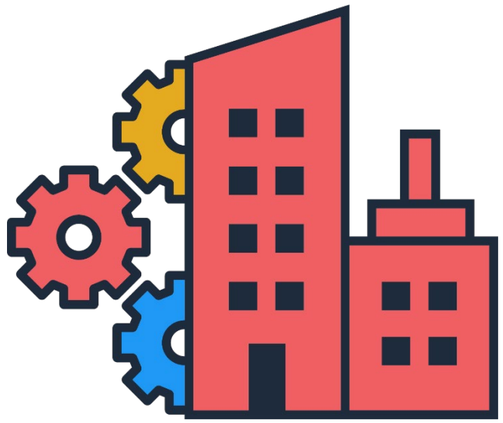
Risikohåndtering

Overvåking og hendelseshåndtering

Måling, evaluering og revisjon

Kompetanse- og kulturutvikling

Kommunikasjon



https://internkontroll-infosikkerhet.difi.no/

digdir.no

Kompetanse- og kulturutvikling

Hvordan arbeider offentlige virksomheter med sikkerhetskompetanse og sikkerhetskultur?

STATSFORVALTNINGEN (2018)

- 27 % klarer ikke å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet
- Virksomhetene arbeider med kompetanseheving, men arbeidet er lite målrettet og ikke tilpasset egenart og behov
- Kun 40 % har kartlagt sikkerhetskulturen

FYLKESKOMMUNER OG KOMMUNER (2020)

- Under halvparten av små og mellomstore kommuner gjennomfører kompetansehevende aktiviteter minst en gang i året
- Manglende kompetanse og forståelse hos medarbeidere og ledere, samt manglende kultur, utgjør hindringer i forbindelse med informasjonssikkerhet

Difi-rapport 2018:4 Arbeidet med informasjonssikkerhet i statsforvaltningen.

Digdir-rapport 2020:3 Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner.

Kompetanse – en del av internkontrollen

Ledelsens styring og oppfølging

Risikovurdering

Risikohåndtering

Overvåking og hendelseshåndtering

Måling, evaluering og revisjon

Kompetanse- og kulturutvikling

Kommunikasjon

Kompetanse og kultur – et kontinuerlig arbeid

- Identifisere behov løpende
- Følge opp identifiserte behov

Kompetanse- og kulturutvikling - veiledning

- Veileder for kartlegging av sikkerhetskultur
- Veileder for kompetanse- og kulturutvikling

https://www.digdir.no/informasjonssikkerhet/kompetanse-og-kulturutvikling-innen-informasjonssikkerhet/2187

Veileder for kartlegging av sikkerhetskultur

Ved å kartlegge sikkerhetskulturen får man

- informasjon som gir økt innsikt i hvordan den menneskelige faktoren påvirker den digitale sikkerheten
- en bedre forståelse av effekten av tiltak som virksomheten gjennomfører for å øke de ansattes bevissthet, holdninger, kunnskaper og adferd innen digital sikkerhet.

Metoden

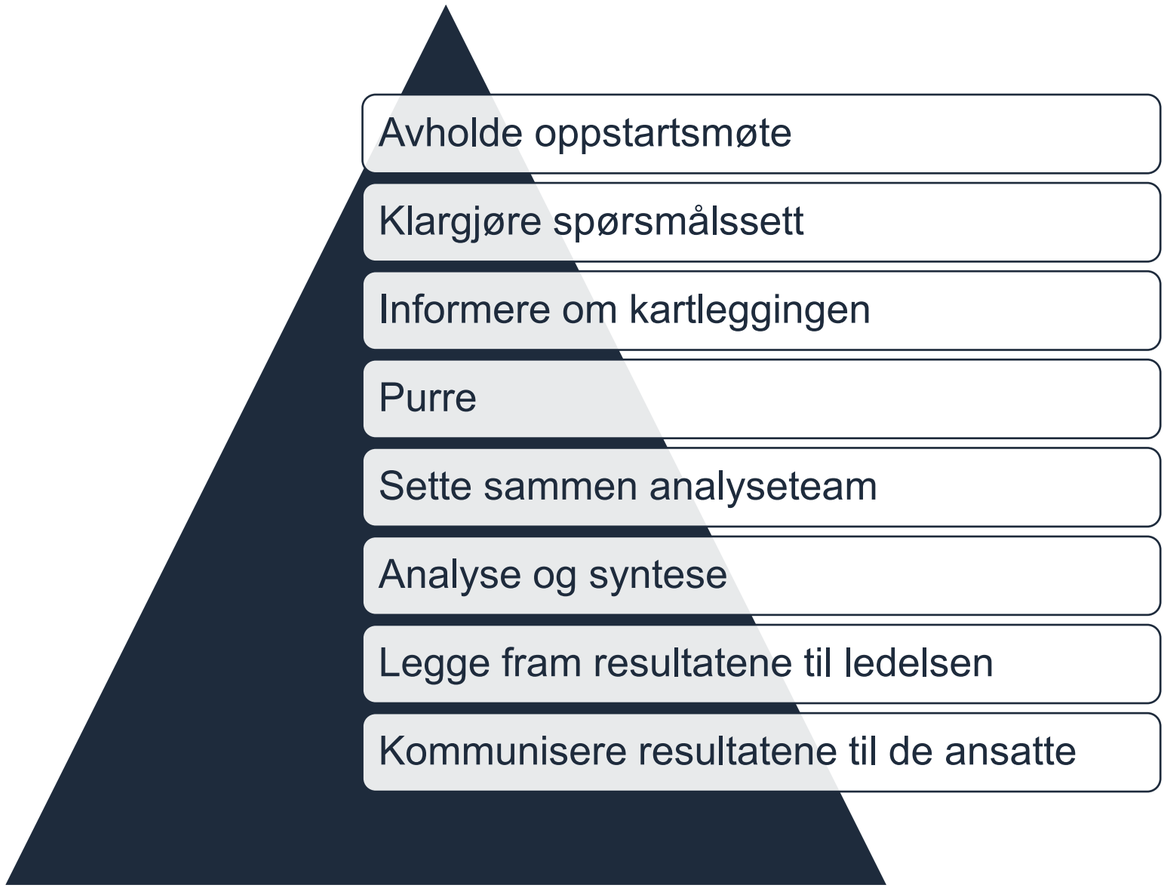
- basert på NorSIS' metode for å måle sikkerhetskulturen i befolkningen
- består av et forslag til plan for kartleggingen, spørsmålssett og maler

Veileder for kompetanse- og kulturutvikling

Veilederen gir

- informasjon om grunnlaget for arbeidet med digital sikkerhetskompetanse og kultur
- anbefalinger til hvordan man kan jobbe med opplæring innen digital sikkerhet
- gode tips til hvordan man lykkes i arbeidet
- tips til hvordan ledelsen kan jobbe med faktorer som påvirker sikkerhetskulturen

Plan for kartleggingen



Kartleggingen skal besvare følgende spørsmål:

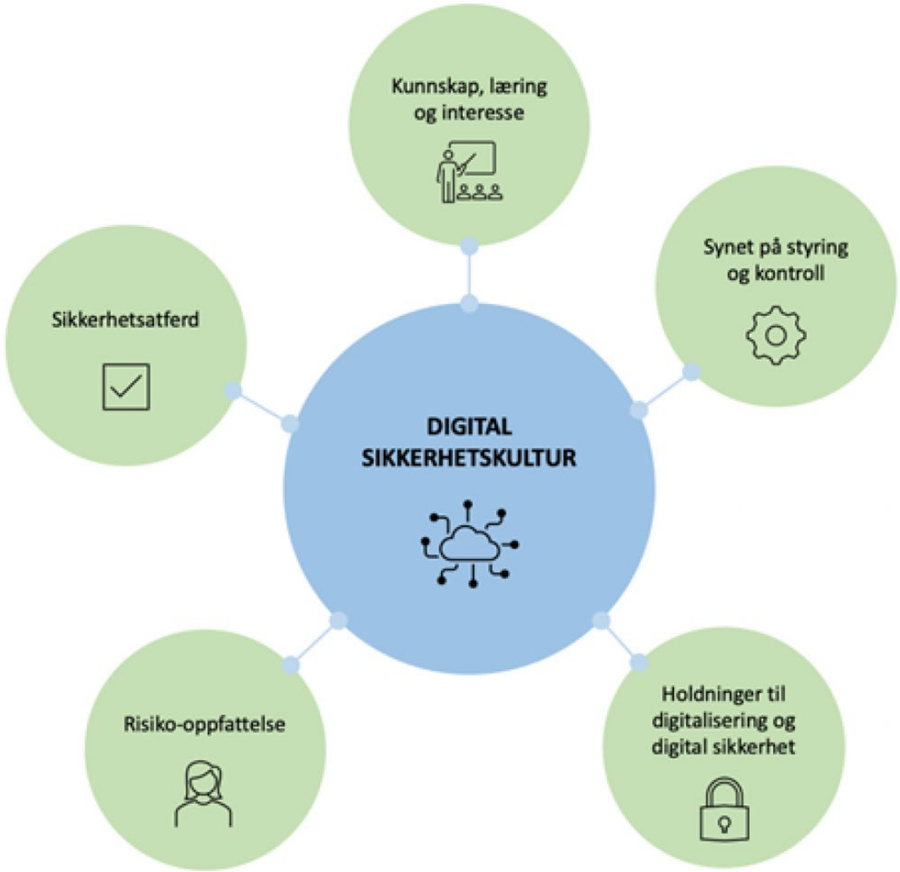
- Hva karakteriserer den digitale sikkerhetskulturen i virksomheten?
- I hvilken grad påvirker opplæring i digital sikkerhet sikkerhetsadferden og sikkerhetskompetansen til alle i virksomheten?
- I hvilken grad tar alle i virksomheten ansvar for den digitale sikkerheten i virksomheten?
- Hvordan forholder alle i virksomheten seg til digitale trusler som kan ramme virksomheten?

Analyse av svarene

- Vurdering av enkeltindikatorer
- Sammenstilling av indikatorer
- Vurdering av kontekst
- Sammenligning av resultater over tid
  - I egen virksomhet
  - Med andre virksomheter

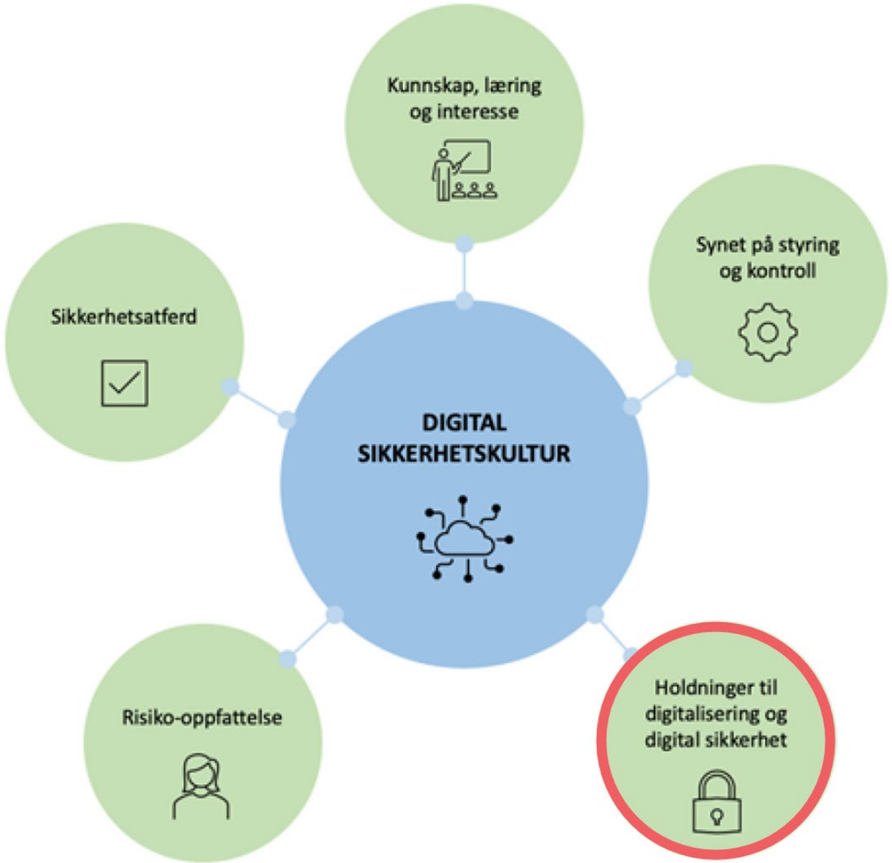
Fem ulike faktorer som påvirker sikkerhetskulturen

- Holdninger til digitalisering og digital sikkerhet
- Risikooppfattelse
- Sikkerhetsadferd
- Kunnskap, læring og interesse
- Synet på styring og kontroll

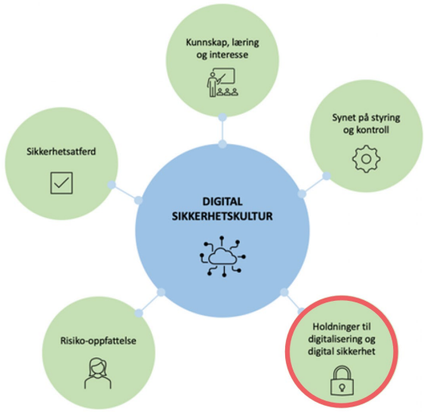


Holdninger til digitalisering og digital sikkerhet

- Beskriver kulturen i organisasjonen
- Kan påvirke bruken av digitale tjenester i positiv eller negativ retning



Digdir



Eksempelspørsmål

8) I hvilken grad opplever du at dine kolleger sier fra til deg om du gjør noe som kan utgjøre en digital risiko for virksomheten? (F.eks. gå fra en datamaskin som ikke er låst med passord)

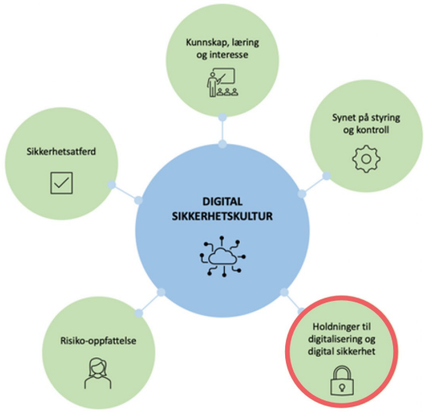
- ○ I svært liten grad
- ○ I ganske liten grad
- ○ I ganske stor grad
- ○ I svært stor grad
- ○ Vet ikke

9) Hvor lett eller vanskelig synes du det er å si fra til en kollega dersom du ser at denne gjør noe som kan utgjøre en digital risiko for virksomheten?

- ○ Det er svært lett å si i fra
- ○ Det er ganske lett å si i fra
- ○ Det er ganske vanskelig å si i fra
- ○ Det er svært vanskelig å si i fra
- ○ Vet ikke

Digdir

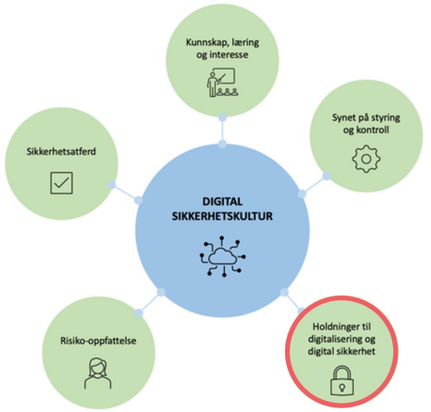
Holdninger til digitalisering og digital sikkerhet



- **Ledelsen bør**
  - beslutte hvilke skrevne og uskrevne normer de ønsker i virksomheten, hvordan de skal kommunisere disse og gå foran med et godt eksempel.
  - kommunisere til organisasjonen hvordan virksomhetens verdier og visjon påvirker den digitale sikkerhetskulturen.
  - kommunisere til organisasjonen hvordan alt henger sammen innen digital sikkerhet, og at det den enkelte gjør innen sikkerhet har betydning for sikkerheten til virksomheten og til fellesskapet.
  - kommunisere til organisasjonen hva virksomheten gjør innen digitalisering og digital sikkerhet og hvorfor dette er viktig for virksomhetens oppdrag.
  - kommunisere til organisasjonen verdien av digitalisering for den enkelte, for virksomheten og for samfunnet, og hvorfor det er viktig å beskytte denne mot digitale risiko.

Digdir

Eksempelspørsmål

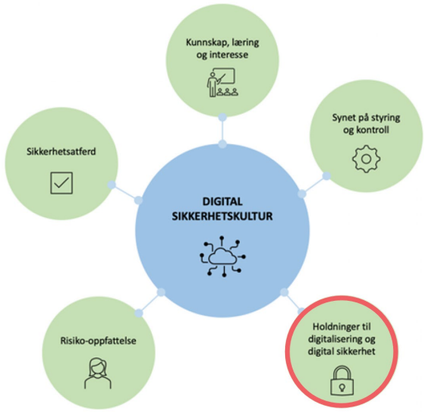


10) I hvilken grad opplever du at ledelsen er gode rollemodeller når det kommer til digital sikkerhet?

- ○ I svært liten grad
- ○ I ganske liten grad
- ○ I ganske stor grad
- ○ I svært stor grad
- ○ Vet ikke

Digdir

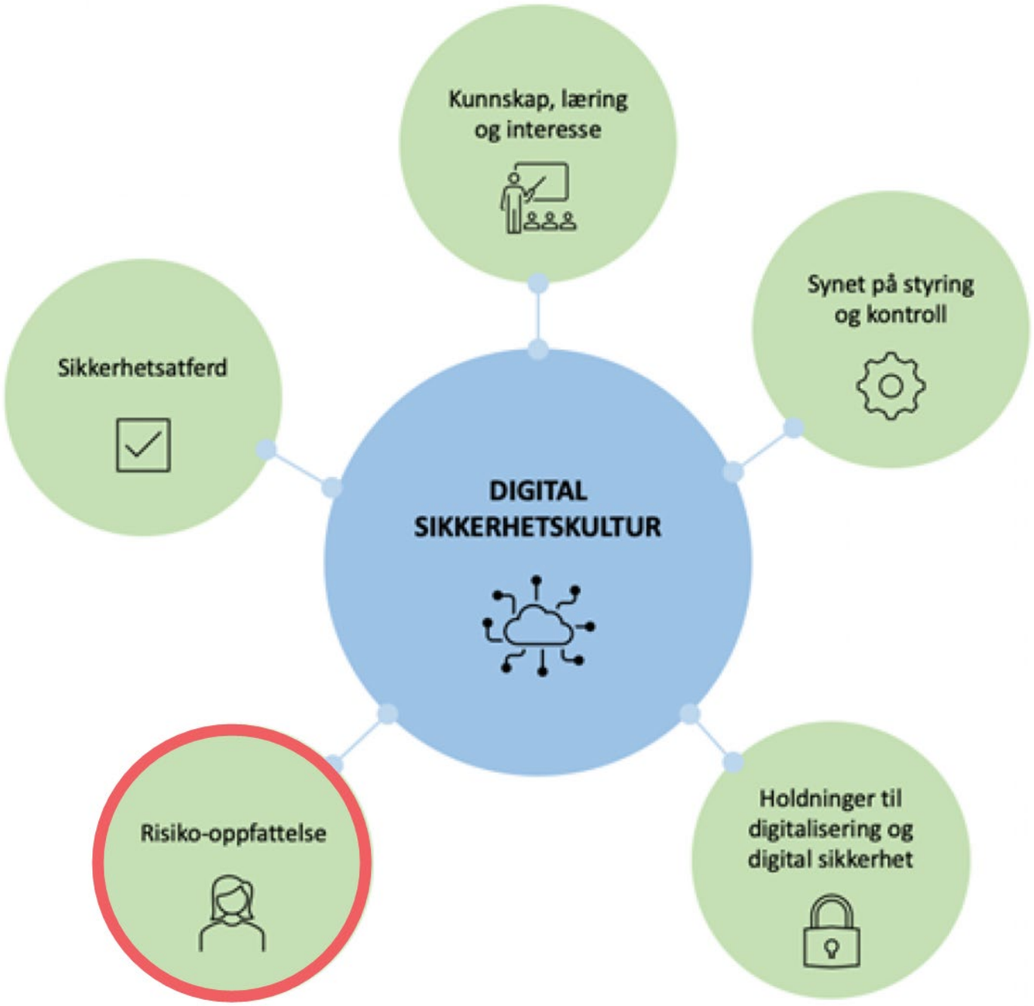
Holdninger til digitalisering og digital sikkerhet



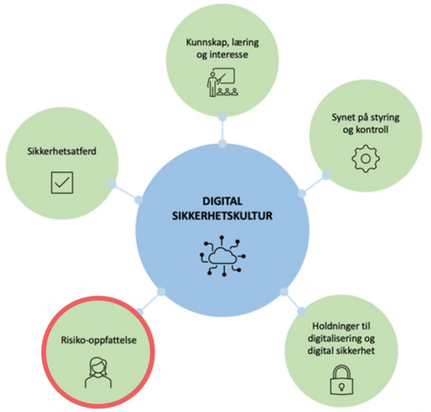
- **Ledelsen bør**
  - beslutte hvilke skrevne og uskrevne normer de ønsker i virksomheten, hvordan de skal kommunisere disse og gå foran med et godt eksempel.
  - kommunisere til organisasjonen hvordan virksomhetens verdier og visjon påvirker den digitale sikkerhetskulturen.
  - kommunisere til organisasjonen hvordan alt henger sammen innen digital sikkerhet, og at det den enkelte gjør innen sikkerhet har betydning for sikkerheten til virksomheten og til fellesskapet.
  - kommunisere til organisasjonen hva virksomheten gjør innen digitalisering og digital sikkerhet og hvorfor dette er viktig for virksomhetens oppdrag.
  - kommunisere til organisasjonen verdien av digitalisering for den enkelte, for virksomheten og for samfunnet, og hvorfor det er viktig å beskytte denne mot digitale risiko.

Risiko-oppfattelse

- Viser hvordan de ansatte forholder seg til risiko
- Gir kunnskap om hvilke tiltak man bør sette inn
- Man bør arbeide for at hele organisasjonen har en lik oppfatning av risiko



Digdir

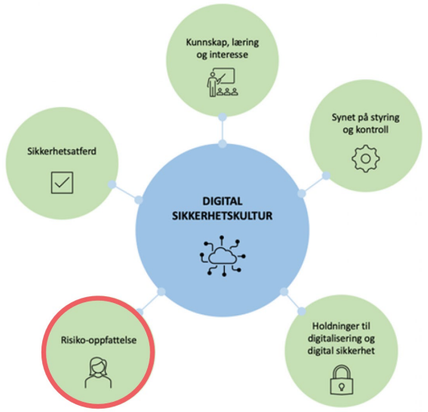


Eksempelspørsmål

12) I hvilken grad er du bekymret for at det følgende skal hende deg?

	I svært liten grad	I ganske liten grad	I ganske stor grad	I svært stor grad	Vet ikke
At jeg skal bli hetset eller mobbet på nett pga. min stilling	○	○	○	○	○
At jeg skal få virus el. på arbeidsgivers datautstyr	○	○	○	○	○
At jeg skal bli lurt til å gi fra meg informasjon	○	○	○	○	○
At min virksomhet skal bli utsatt for målrettede digitale angrep fra eksterne aktører	○	○	○	○	○
At min virksomhet skal bli utsatt for digitale angrep fra utro tjenere	○	○	○	○	○
At min virksomhet skal bli utsatt for svikt i digitale systemer på bakgrunn av utilsiktede feil	○	○	○	○	○

Digdir

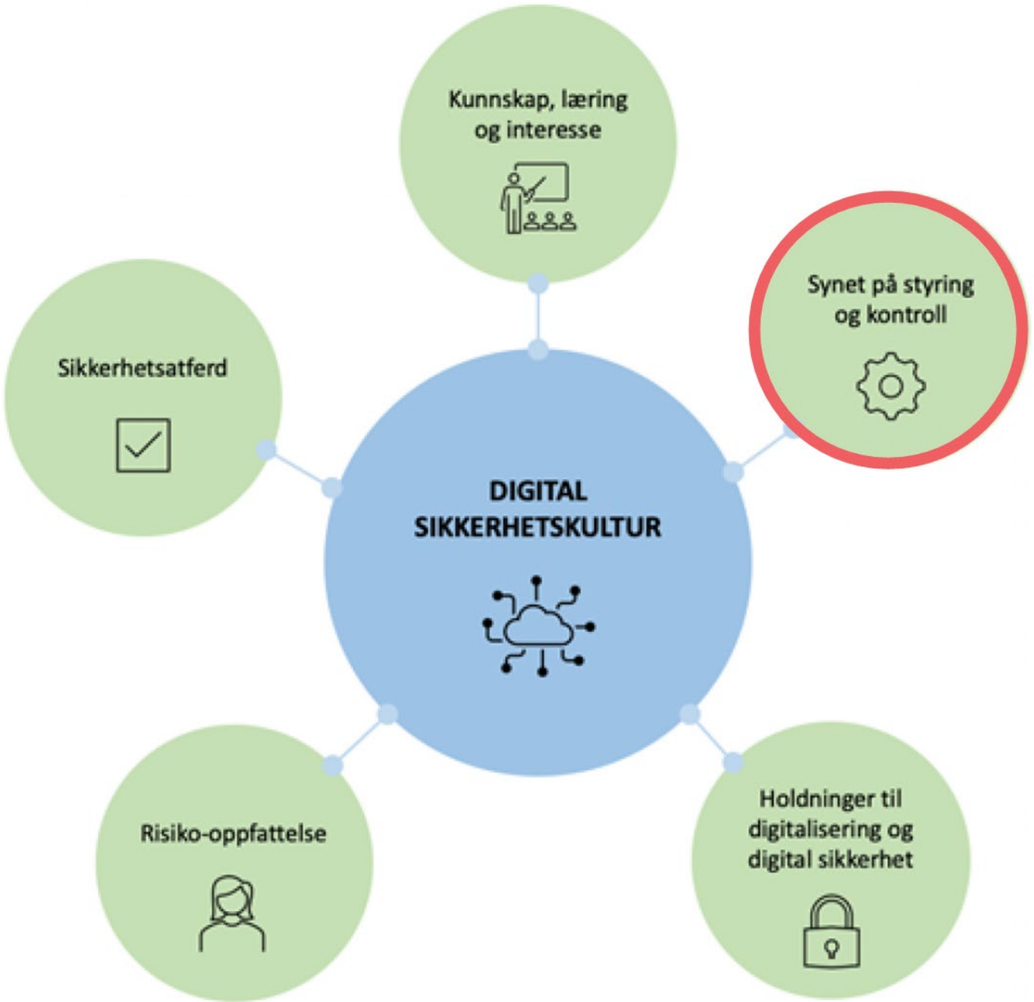


Risiko-oppfattelse

- **Ledelsen bør:**
  - kommunisere til organisasjonen fakta omkring sikkerhetshendelser som rammer virksomheten, andre relevante virksomheter eller samfunnet for øvrig.
  - kommunisere til organisasjonen hva som gjøres for å beskytte virksomheten, de ansatte og brukere av virksomhetens tjenester, mot digital risiko.
  - kommunisere til organisasjonen hvordan de skal gjøre risikovurderinger og fortløpende tolke risikosituasjonen.
  - sørge for at organisasjonen har kunnskap, metodikk og verktøy for å vurdere og håndtere den risiko de er ansvarlig for, og den risiko de må vurdere i det daglige.

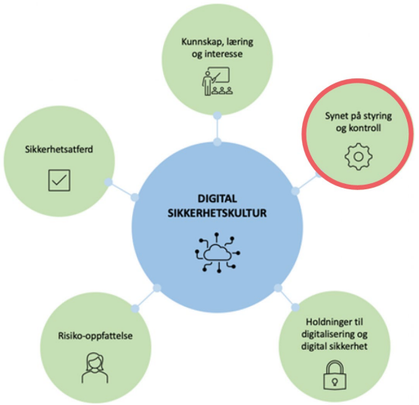
Synet på styring og kontroll

- Viser om organisasjonen kjenner og følger føringene fra ledelsen



Digdir

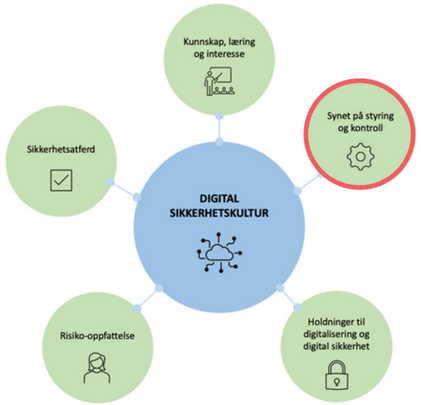
Eksempelspørsmål



15) Har virksomheten din regler for digital sikkerhet?

○ Ja ○ Nei ○ Vet ikke

Digdir

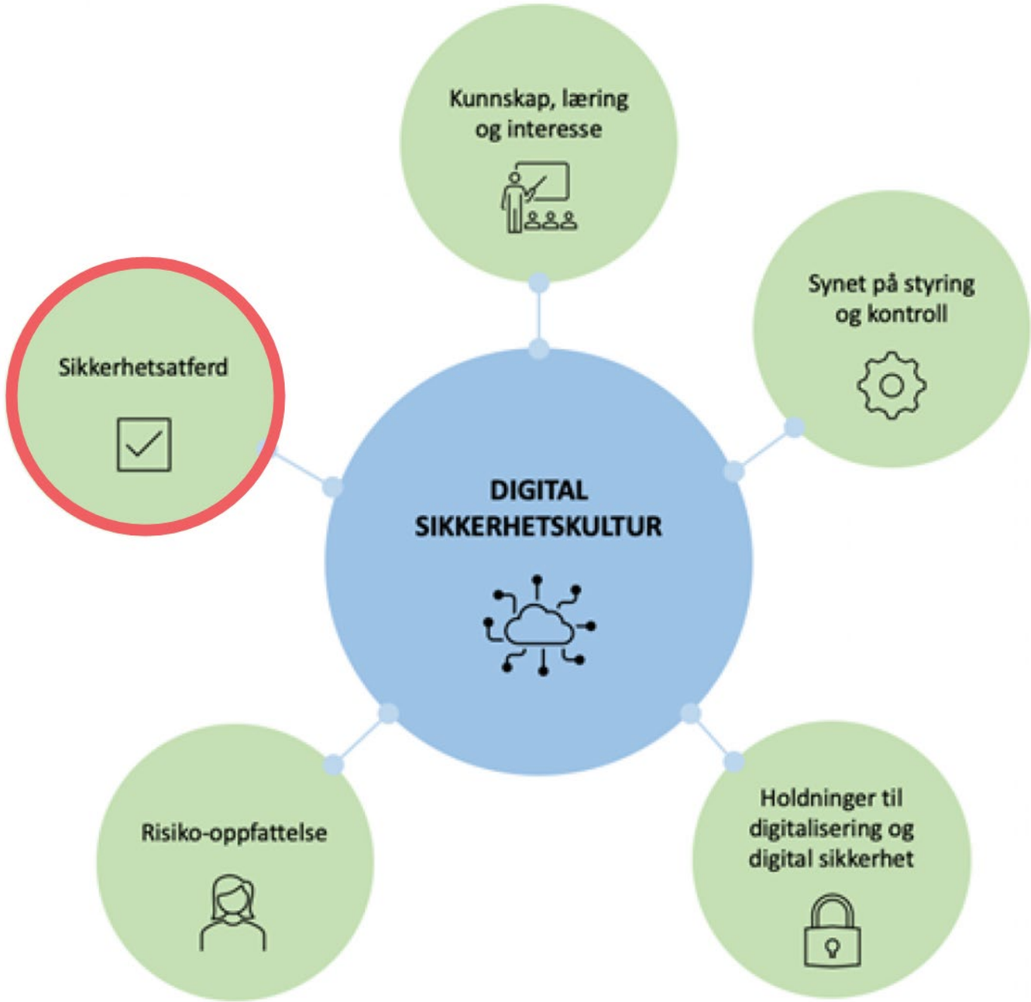


Synet på styring og kontroll

- **Ledelsen bør:**
  - legge føringer (for eksempel regler og retningslinjer) som er forståelige og mulige for menneskene i organisasjonen å følge.
  - igangsette tiltak for å øke organisasjonens motivasjon til å sette seg inn i føringene, og å følge disse. Sanksjoner og incentiver bør velges med omhu, og effekten av dem bør kartlegges og evalueres.
  - etablere varslingsordninger slik at organisasjonen kan varsle om hendelser og andre sikkerhetsrelaterte forhold. Det bør vurderes om ordningen skal legge til rette for anonym varsling.
  - kommunisere til organisasjonen hvordan digital sikkerhet styres, hvem som setter føringene, hva som er den enkeltes ansvar, hvor den enkelte kan finne informasjon etc.
  - kommunisere relevante føringer til organisasjonen ved tilsettinger, når reglene endres eller når endringer i risikobildet tilsier at føringene bør kommuniseres på ny.

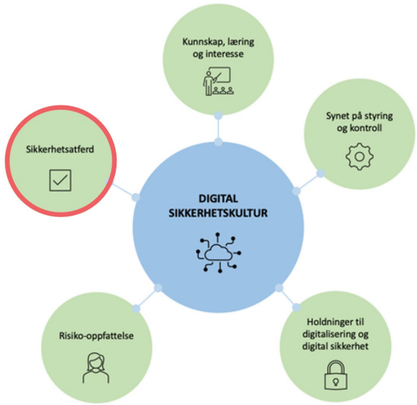
Sikkerhetsadferd

- Kartlegger adferdsmønstre for å:
  - lære mer om hva de ansatte faktisk gjør i ulike situasjoner
  - etterprøve om organisasjonen som helhet følger føringene som blir gitt
  - vurdere effekten av opplæring og holdningskampanjer



Digdir

Eksempelspørsmål

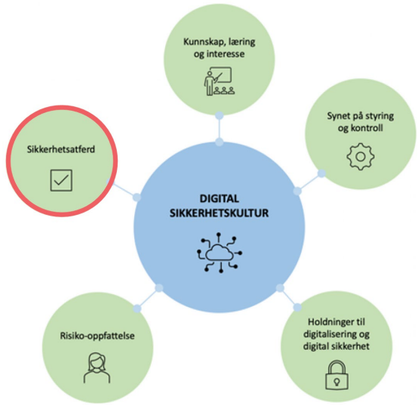


26) I hvilken grad poster du informasjon om arbeidet ditt i sosiale medier?

- ○ I svært liten grad
- ○ I ganske liten grad
- ○ I ganske stor grad
- ○ I svært stor grad
- ○ Vet ikke

Digdir

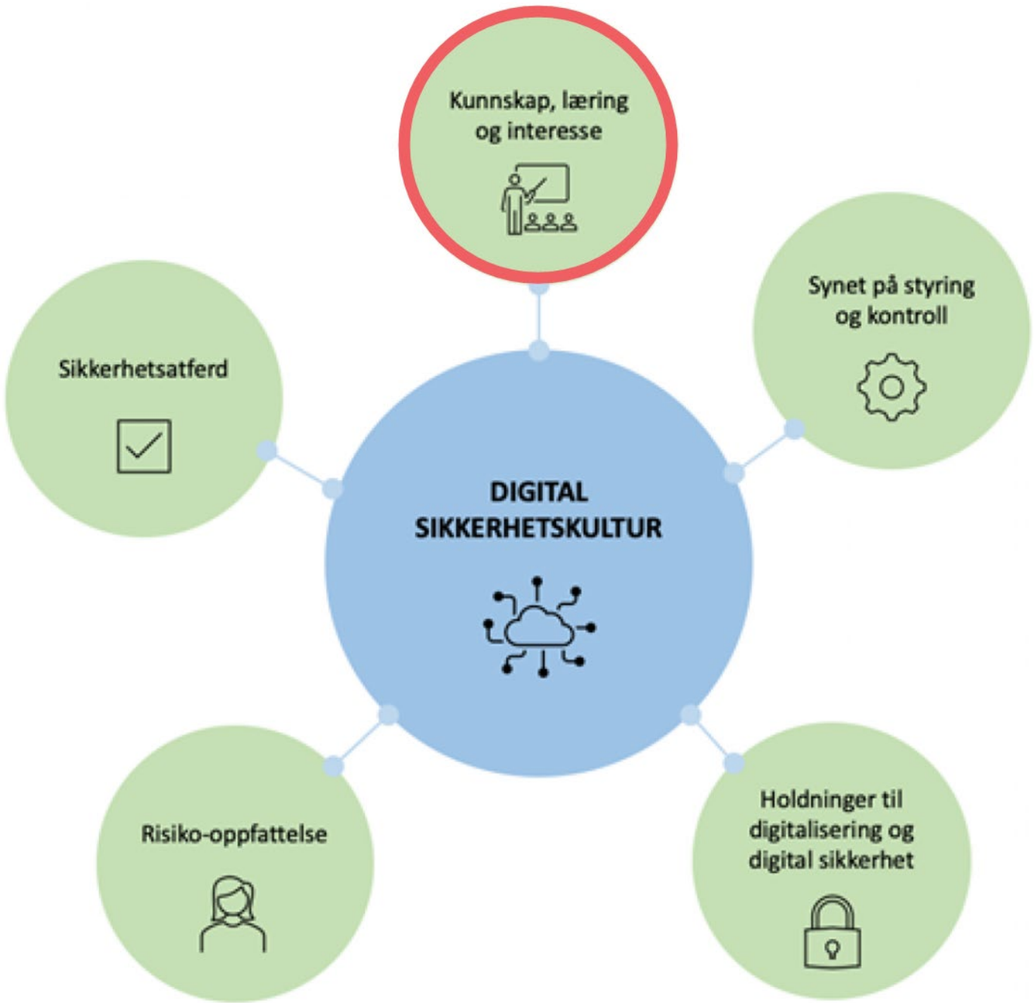
Sikkerhetsadferd



- **Ledelsen bør:**
  - fastsette adferdsnormer, basert på hvilken adferd som er ønskelig, og gå foran med et godt eksempel.
  - innføre tiltak som motiverer organisasjonen til å etablere ønskede adferdsnormer.
  - innføre kompetanseheving basert på hva som er ønskede adferdsnormer.
  - fokusere på den enkeltes mestringsfølelse, ikke bare nødvendig kunnskap.
  - fokusere på at adferdsnormene må være mulig å gjennomføre for menneskene i organisasjonen. Det bør tas hensyn til at menneskene på ulike arbeidsplasser har ulik kompetansebakgrunn og -sammensetting.
  - legge til rette for at organisasjonen kan gjennomføre øving og trening innen digital sikkerhet. Dette bør tilrettelegges for den enkelte, for team og hele organisasjonen.

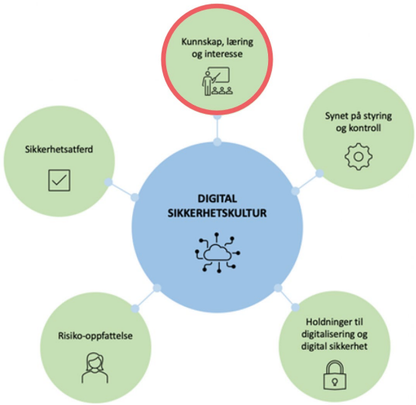
Kunnskap, læring og interesse

- Hvordan lærer de ansatte om digital sikkerhet?
- Kartlegger:
  - kunnskapen i organisasjonen
  - Hvordan læringsprosesser skjer
- Gir grunnlag for å evaluere effekten av kunnskapsheving



Digdir

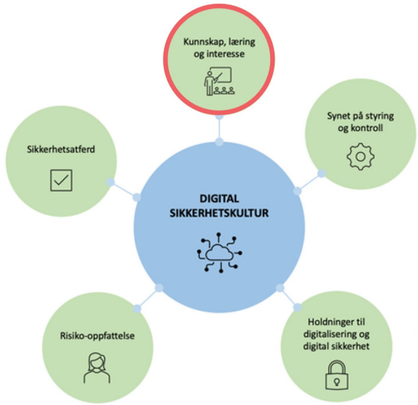
Eksempelspørsmål?



30) Har virksomheten tilbudt opplæring i digital sikkerhet i løpet av de to siste årene?

- ○ Ja, og jeg har deltatt
- ○ Ja, og jeg har ikke deltatt
- ○ Nei
- ○ Vet ikke

Digdir



Kunnskap, læring og interesse

- **Ledelsen bør:**
  - beslutte hva det er behov for at organisasjonen kan om digital sikkerhet, og utarbeide kompetanseplaner og opplæringsplaner.
  - sørge for at alle får et felles kunnskapsgrunnlag ved ansettelse.
  - sørge for jevnlig kunnskapsheving når noe skjer, basert på sikkerhetshendelser, ved omorganiseringer eller ved innføring av nye digitale systemer.
  - stimulere til læringsprosesser som er effektive og som passer virksomheten (For eksempel e-læring, klasseromsundervisning eller foredrag).

Helhetlig arbeid med kompetanse- og kulturutvikling

Helhetlig arbeid med kompetanse- og kulturutvikling

- Kartlegge behov
- Velge målgruppe
- Ta i bruk passende tiltak
- Tenke helhetlig
- Måle effekt
- Etablere forvaltningsregime

Digitaliseringsdirektoratets tilbud

- Internkontroll i praksis – informasjonssikkerhet
- Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet
- Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet
- Dilemmatrening
- E-læringskurs «Er det sikkert?» på statens læringsplattform

digdir.no/infosikkerhet

infosikkerhet@digdir.no

digdir.no

Digitaliseringsdirektoratet

postmottak@digdir.no

22 45 10 00

Postboks 1382 Vika, 0114 Oslo

Besøksadresser:

Industriveien 1, 8900 Brønnøysund

Skrivarevegen 2, 6863 Leikanger

Grev Wedels Plass 9, 0151 Oslo