# Forbedre kommunikasjon og samarbeid mellom et sikkerhetsoperasjonssenter (SOC) og en kommune


**Emina Engh (23)**

**MSc Information Security**
**NTNU**



**Camilla Molland (23)**

**MSc Information Security**
**NTNU**



**Nora Altamimi (23)**

**MSc Information Security**
**NTNU**

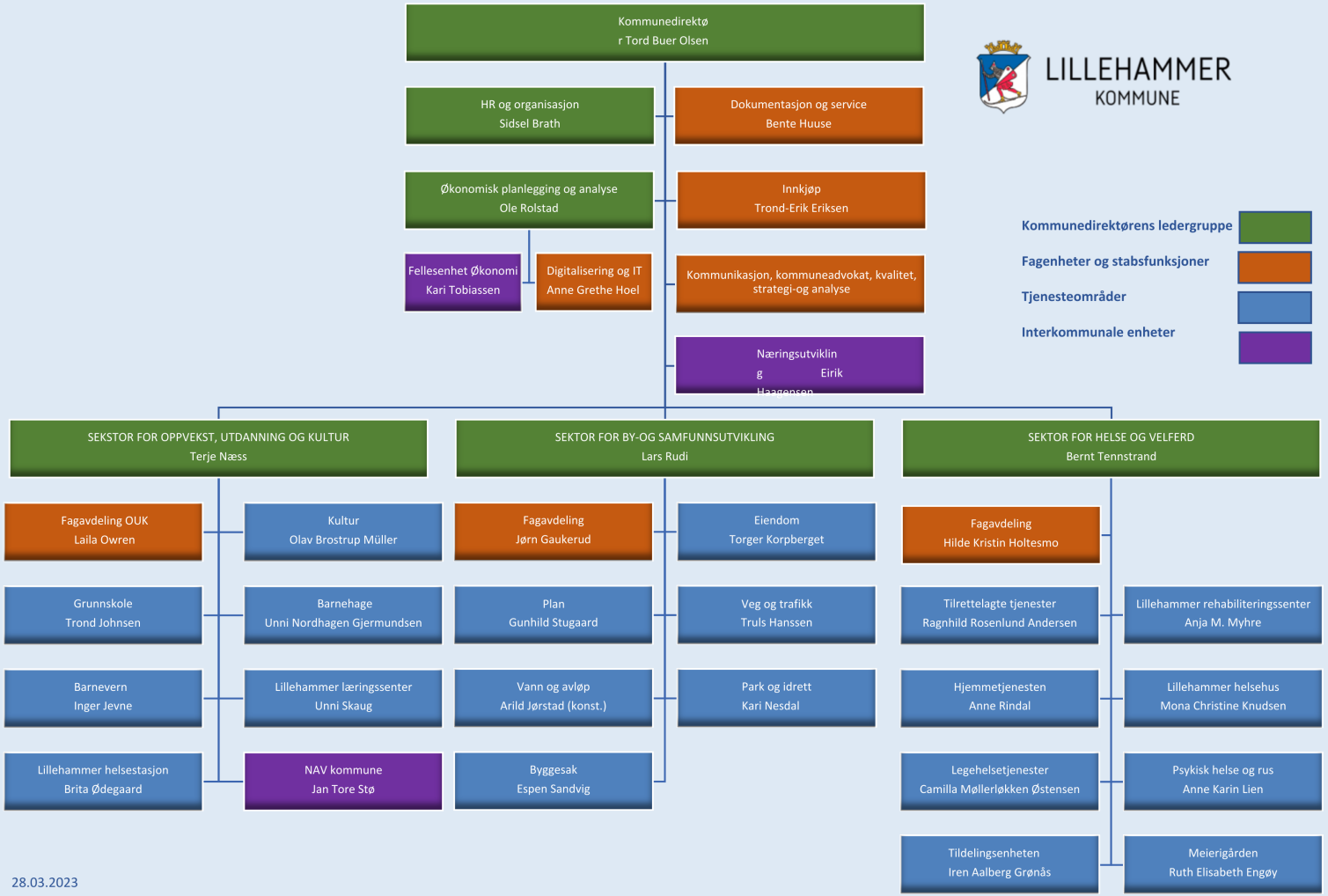


**Katrine B. Lyngen (23)**

**Security Trainee**
**HDO**

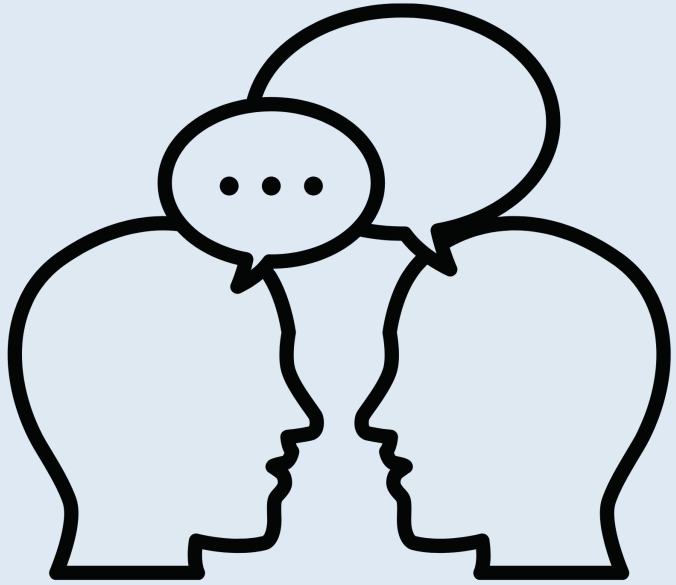
# Bakgrunn

- Oppdragsgiver Ikomm
- Etablere ekstern SOC
- Utfordringer




28.03.2023
Utarbeidet av HR og organisasjon

# Oppgaven



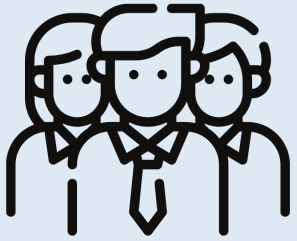
Kommunikasjon

Samarbeid

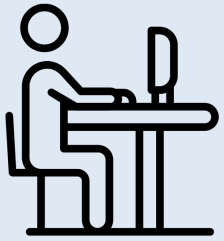
Anbefalinger

# Metodikk

## Spørreundersøkelse



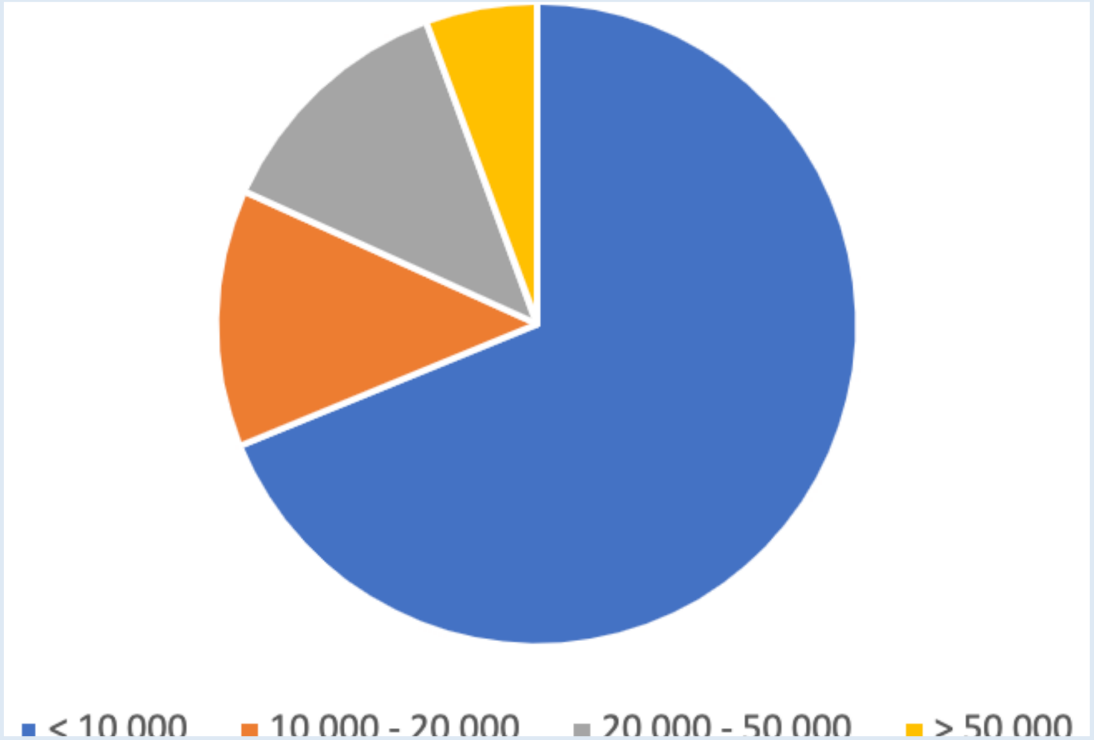
Kommuneansatte - 314



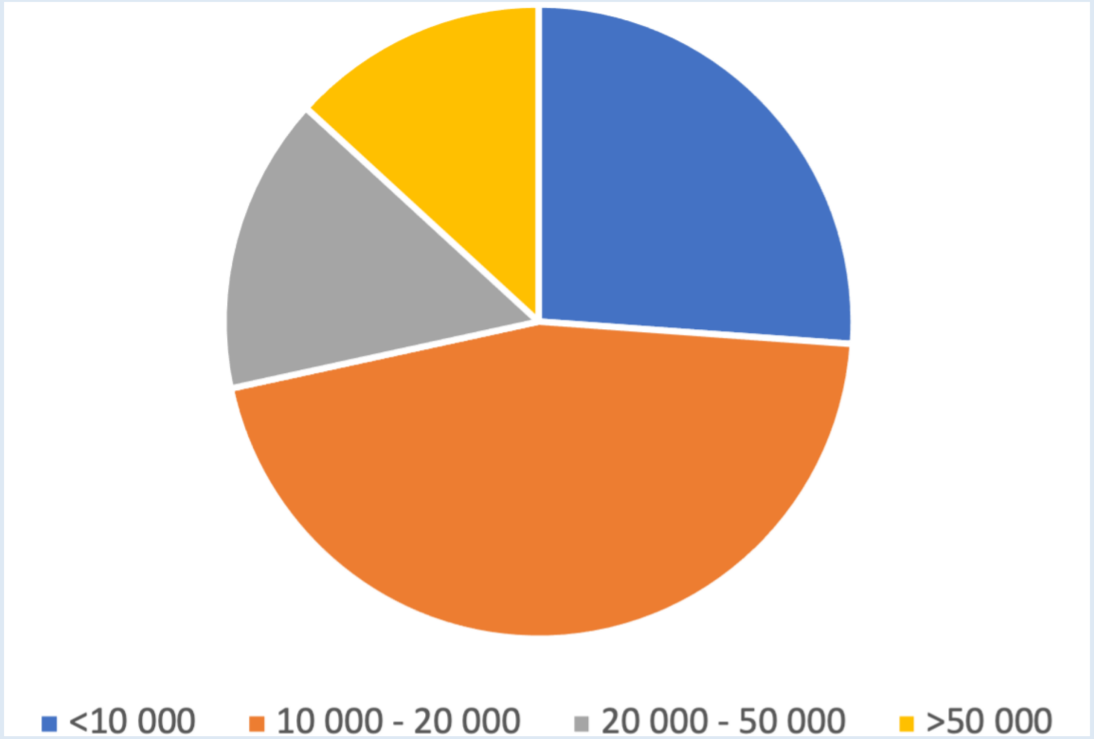
IT - 59

## Intervju - 13

# Resultat spørreundersøkelse - Kommuneansatte

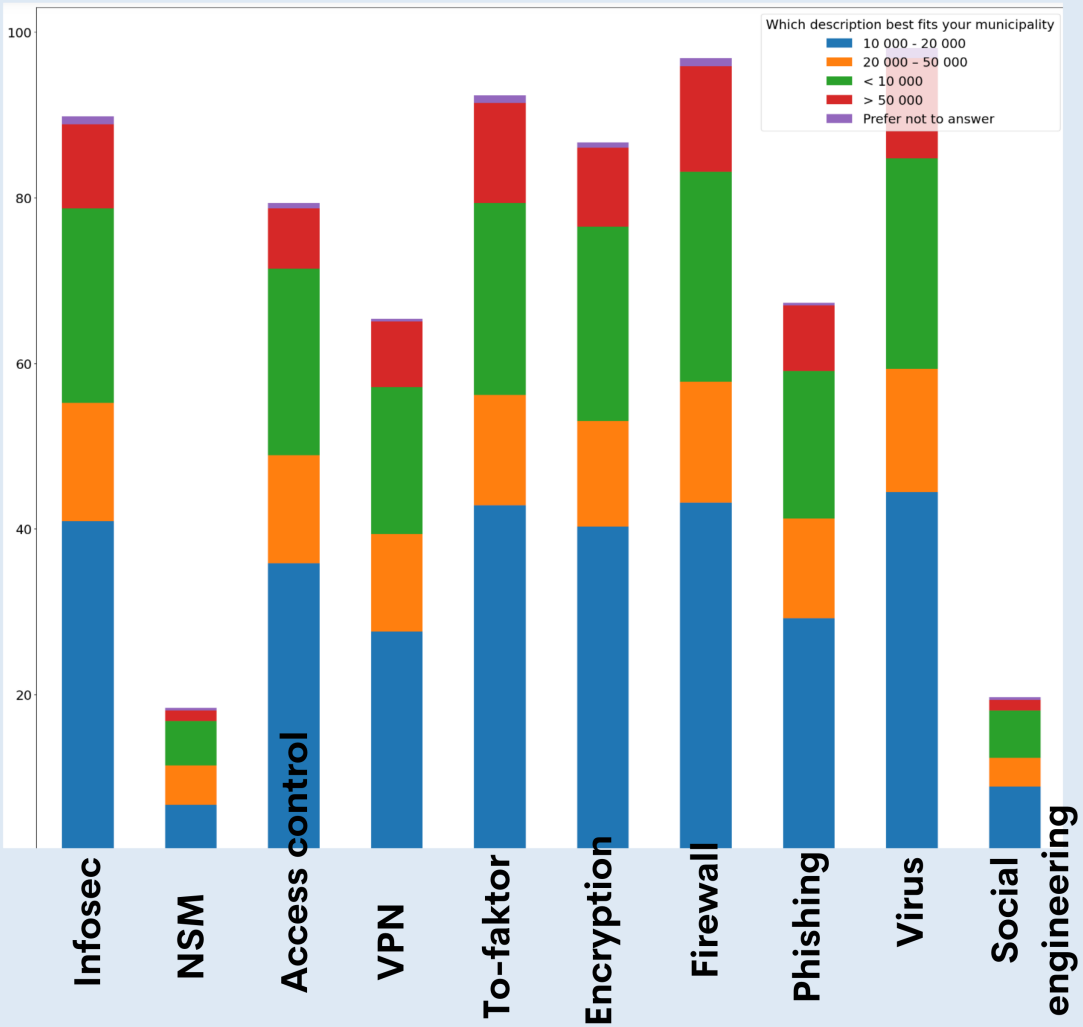



Distribusjon av kommuner

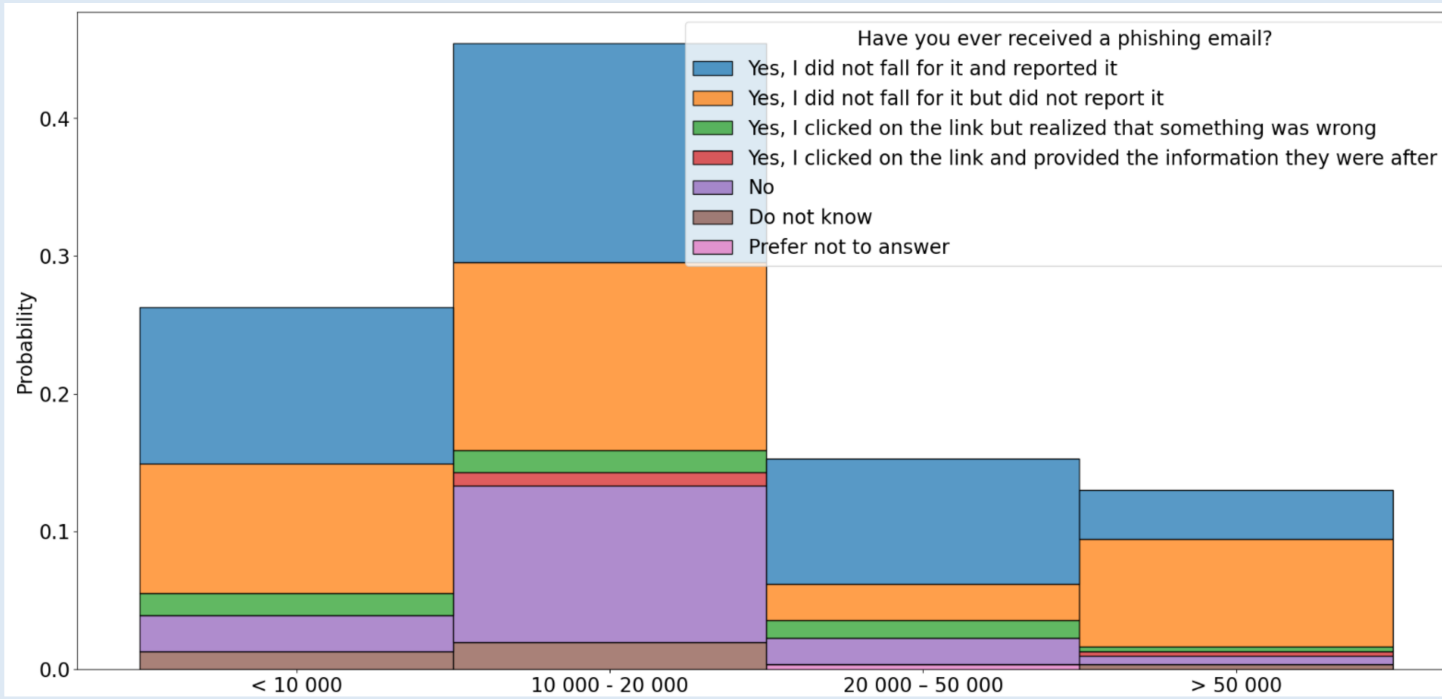



Distribusjon av kommuner fra undersøkelse

# Analyse

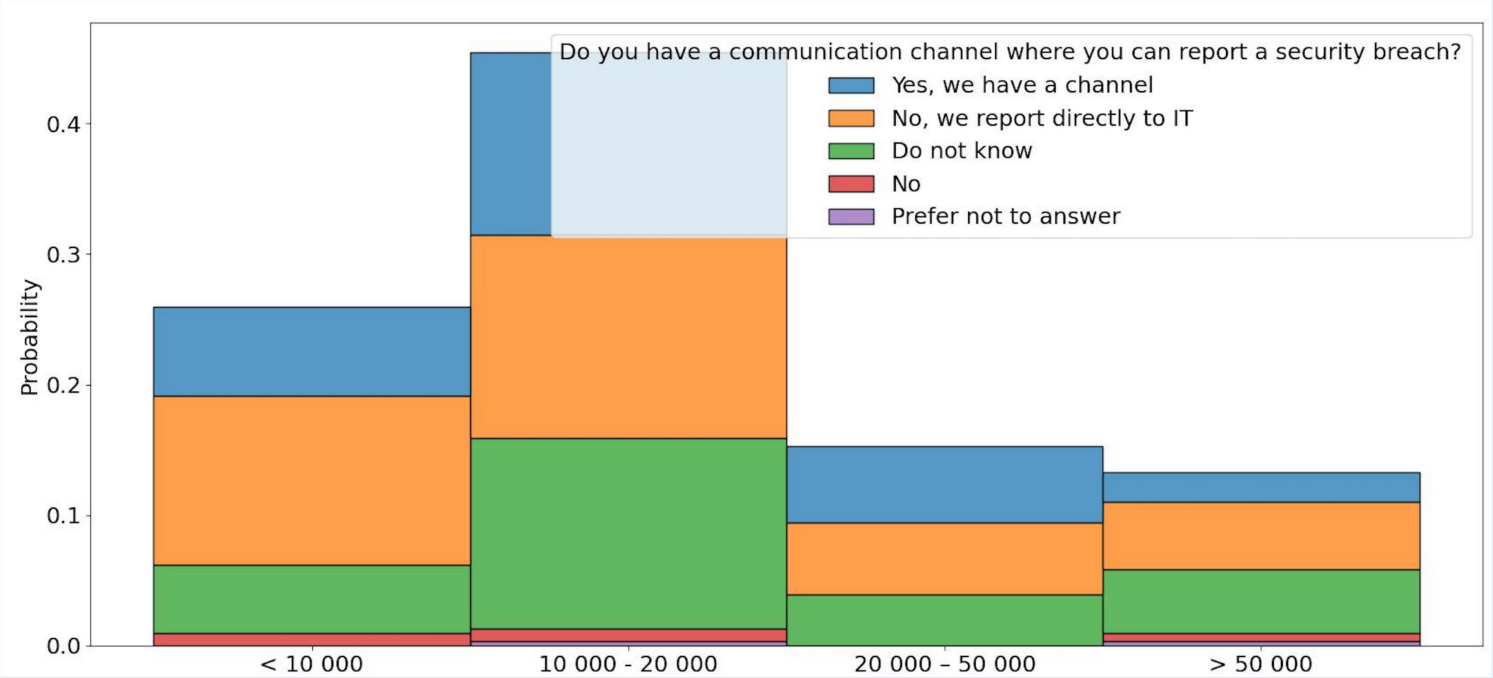



**Hvor mange av disse begrepene er du kjent med?**

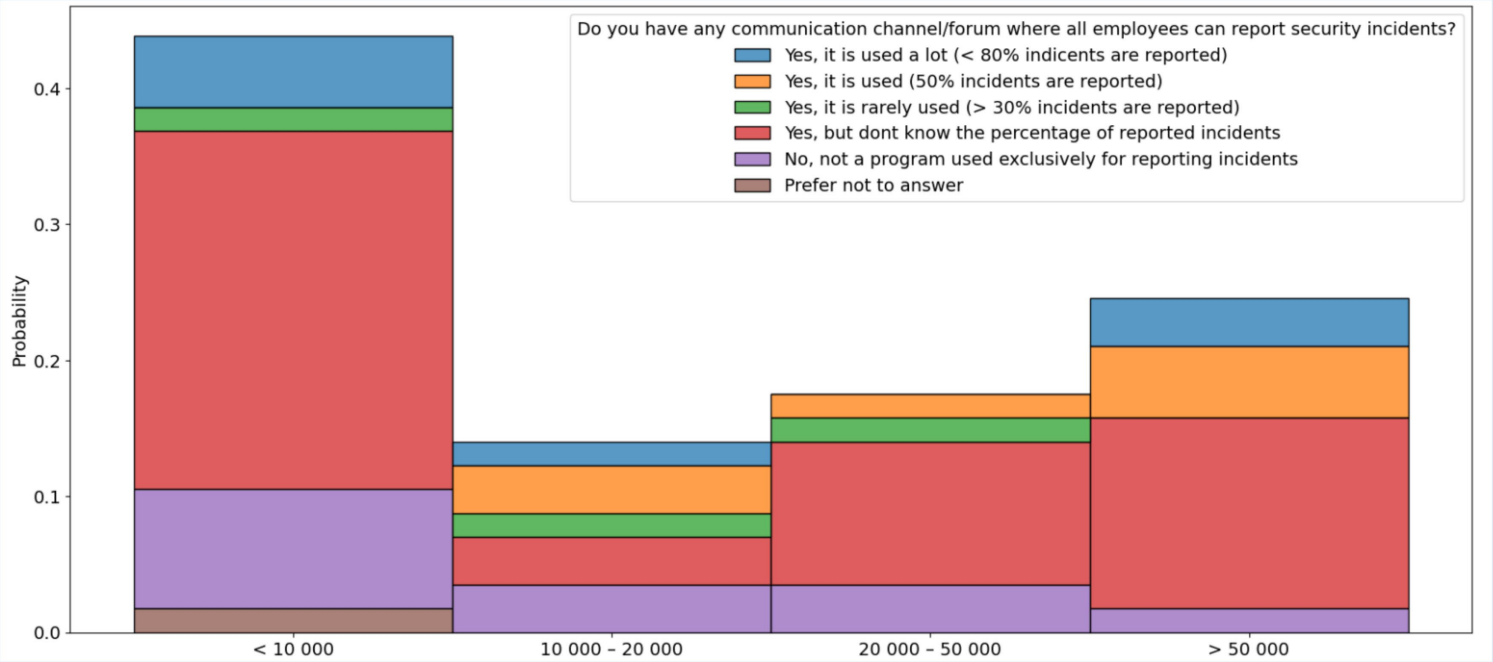



**Har du noen gang fått en phishing mail?**

**Kommuneansatte**

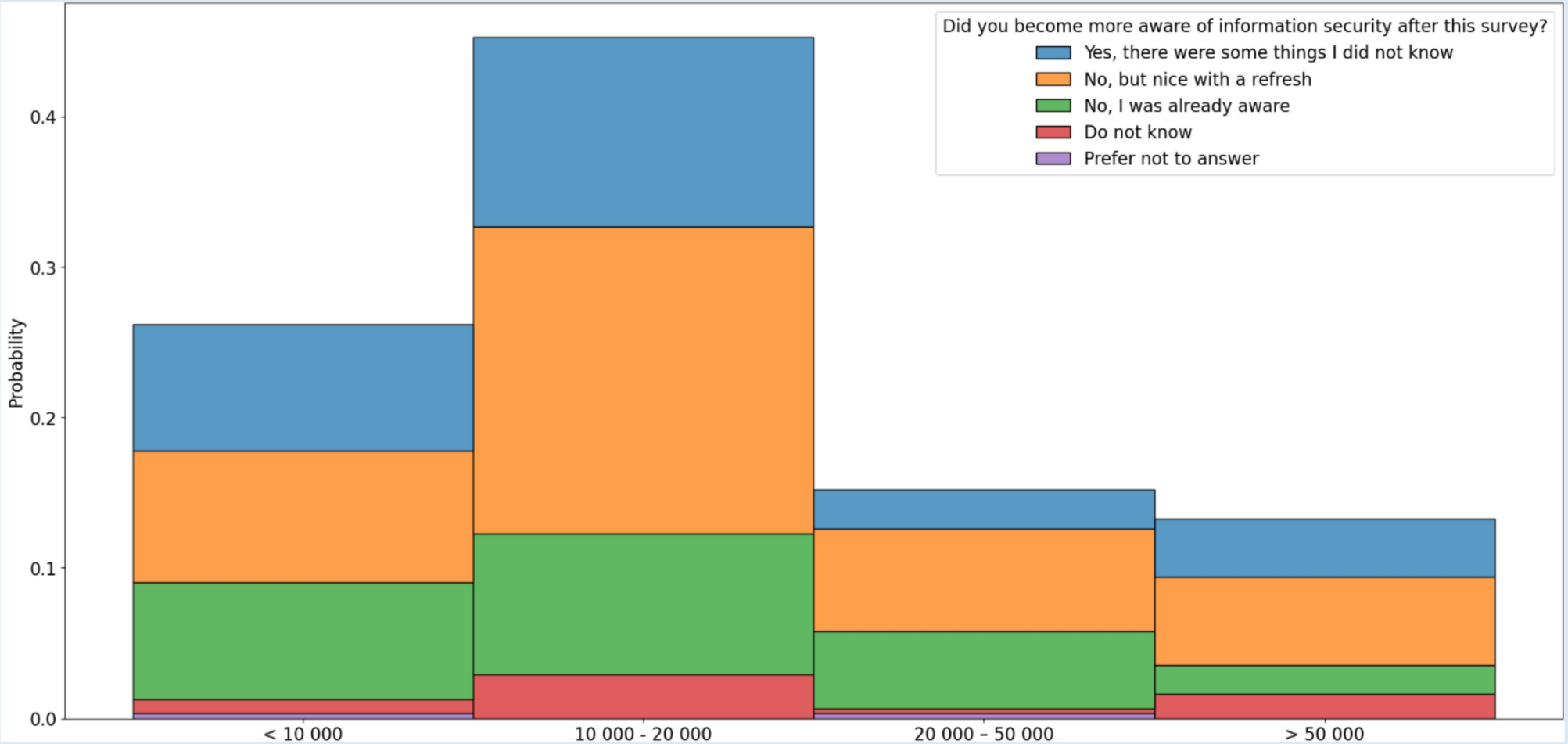



# Har dere noen kommunikasjonskanal brukt for å melde inn sikkerhetsbrudd?

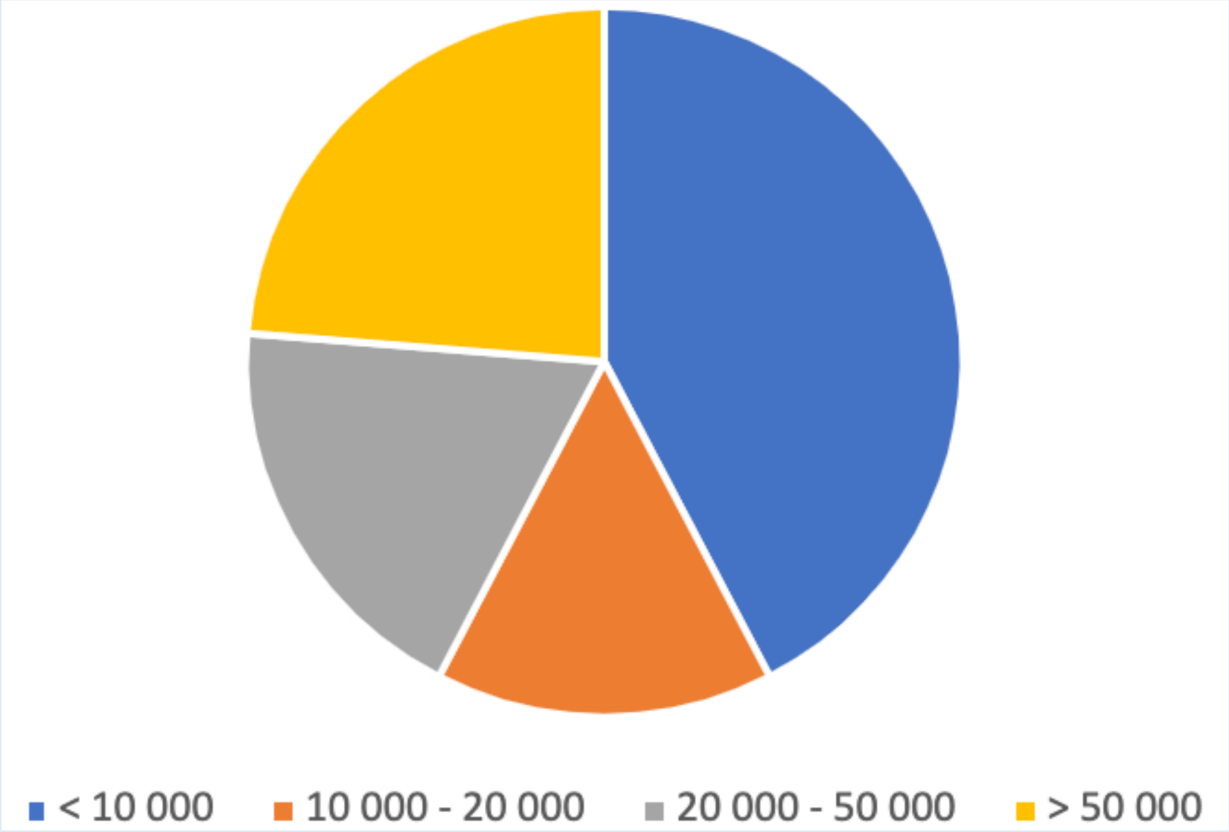



**IT personell**

# Ble du noe mer bevisst på informasjonssikkerhet etter denne undersøkelsen?

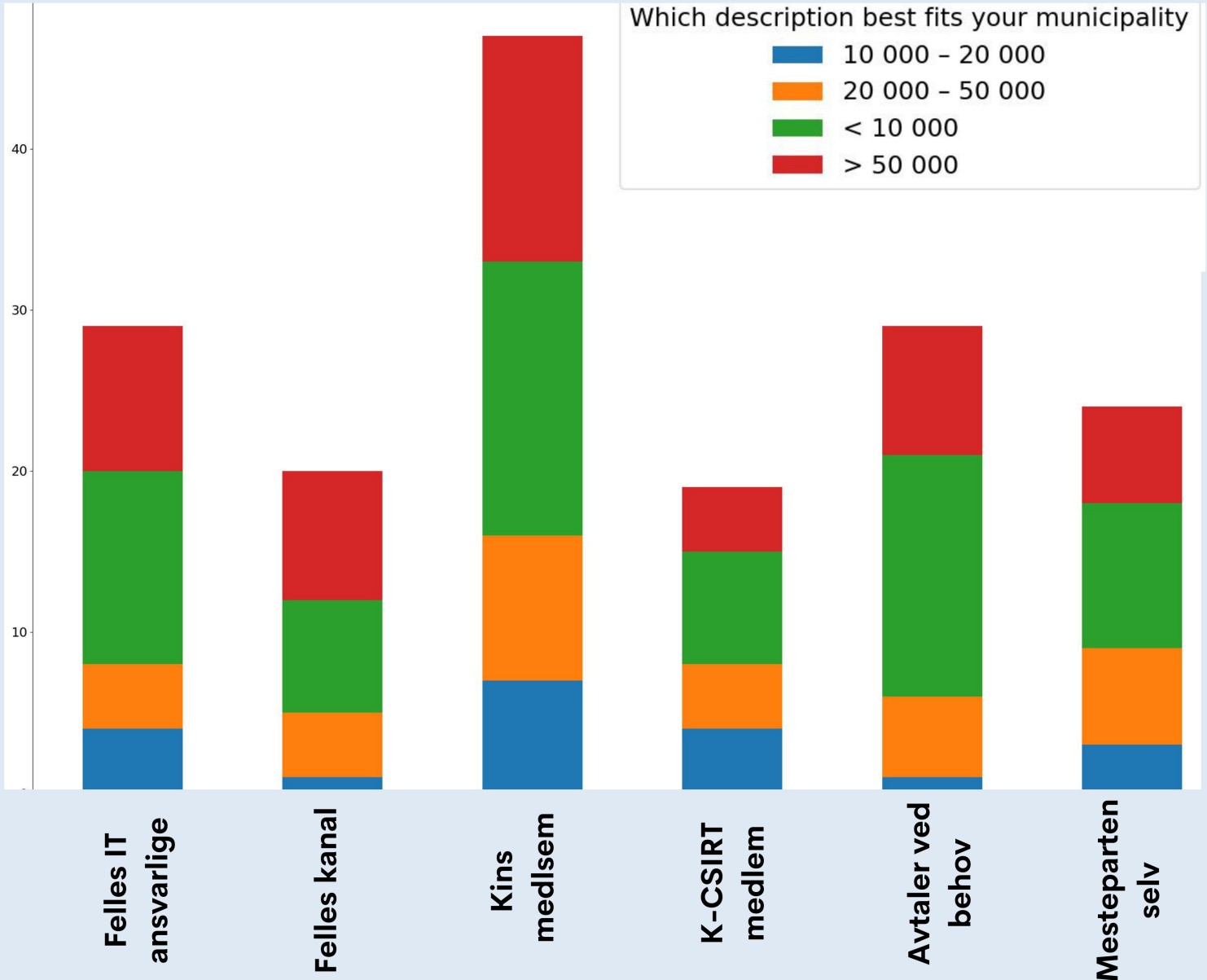


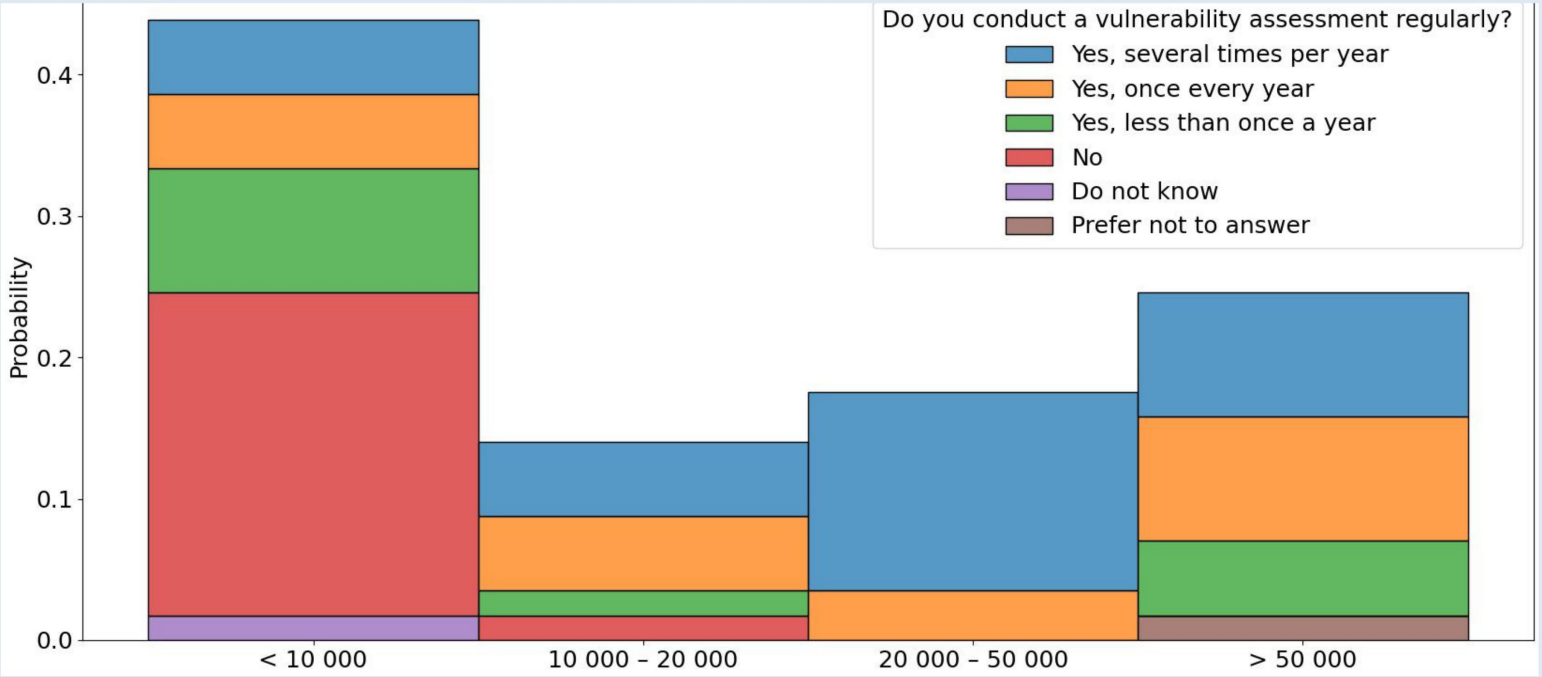
# Resultat spørreundersøkelse - IT personell



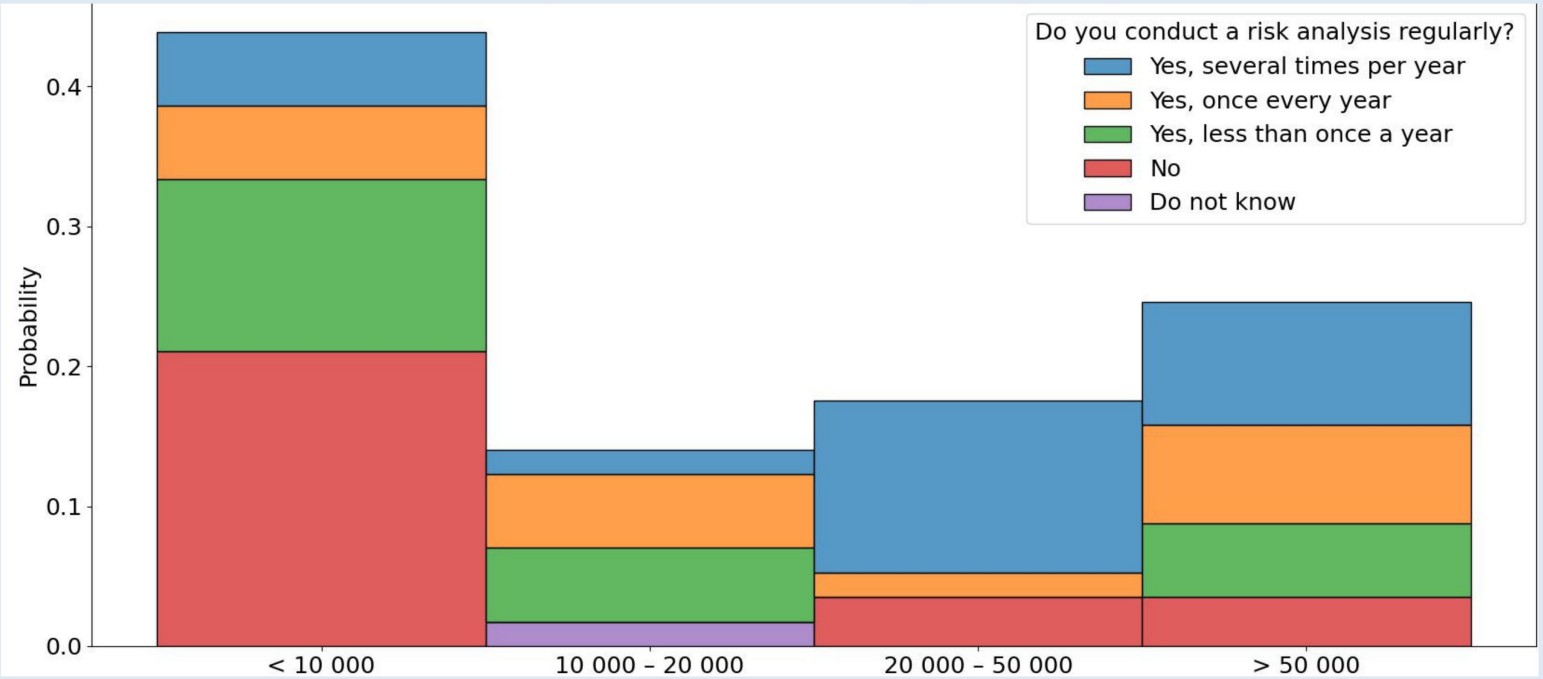

**Distribusjon av kommuner fra undersøkelse**

# Hvilke av disse gjelder for din kommunes IT-samarbeid?



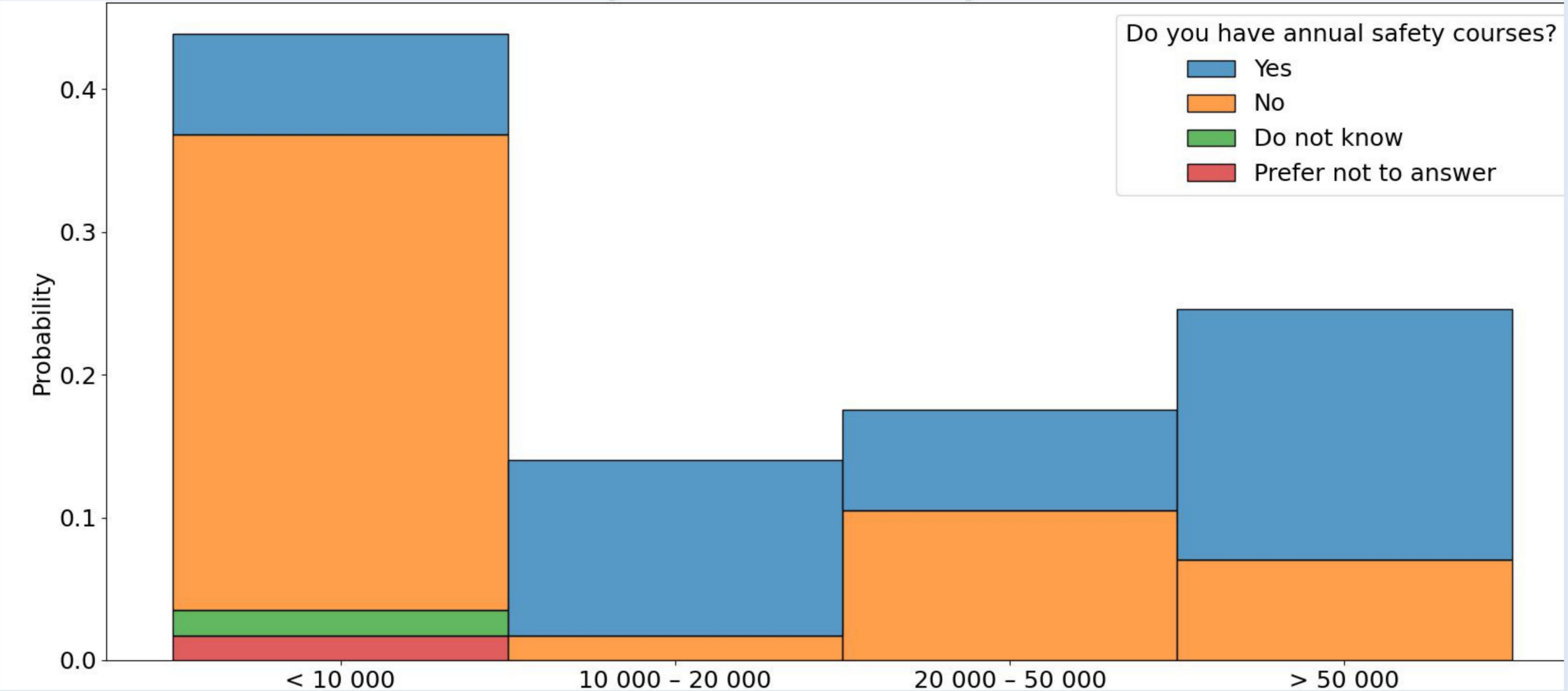



# Gjennomfører dere en sårbarhetskartlegging periodisk?




# Gjennomfører dere en risikovurdering periodisk?

# Har dere årlige sikkerhetskurs?



# Anbefalinger

1.Organisering og kartlegging

2. Kommunikasjon mellom SOC og kommune

3. Ansvarsfordeling

4. Kompetanse en kommune bør ha

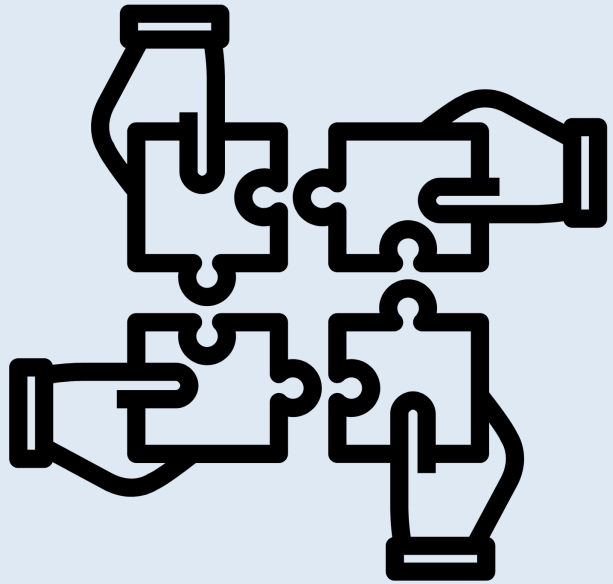
# Anbefalinger

1. **Organisering og Kartlegging**

   **1.1 Interkommunalt samarbeid**

   1.2 Erfaren SOC leverandør

   1.3 Kartlegg nettverkstopologi og systemer



# Anbefalinger

## 2. Kommunikasjon mellom SOC og kommune

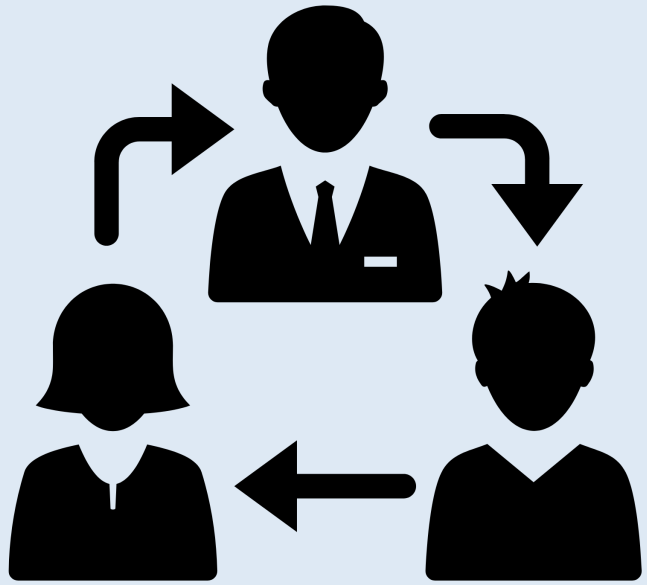
2.1 Trafikklysprotokoll

2.2 To-veis kommunikasjon

**2.3 Identifisere kontaktpersoner og roller**

2.4 Klare kommunikasjonskanaler

2.5 Språkvalg



# Anbefalinger

## 2. Kommunikasjon mellom SOC og kommune

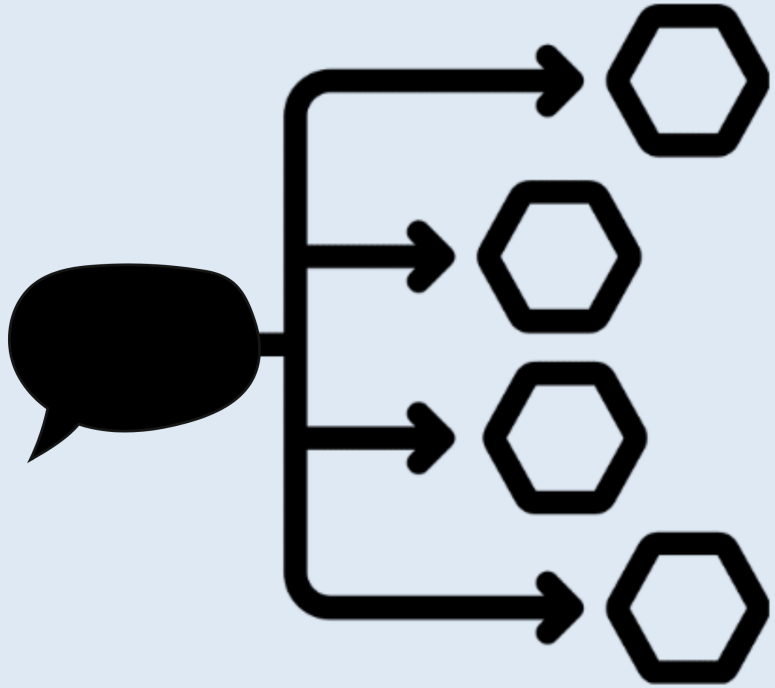
2.1 Trafikklysprotokoll

2.2 To-veis kommunikasjon

2.3 Identifisere kontaktpersoner og roller

**2.4 Klare kommunikasjonskanaler**

2.5 Språkvalg



# Anbefalinger

## 2. Kommunikasjon mellom SOC og kommune

2.1 Trafikklysprotokoll

2.2 To-veis kommunikasjon

2.3 Identifisere kontaktpersoner og roller

2.4 Klare kommunikasjonskanaler

**2.5 Språkvalg**

# Anbefalinger

## 3. Ansvarsfordeling

**3.1 SOC leverer tjenesten**

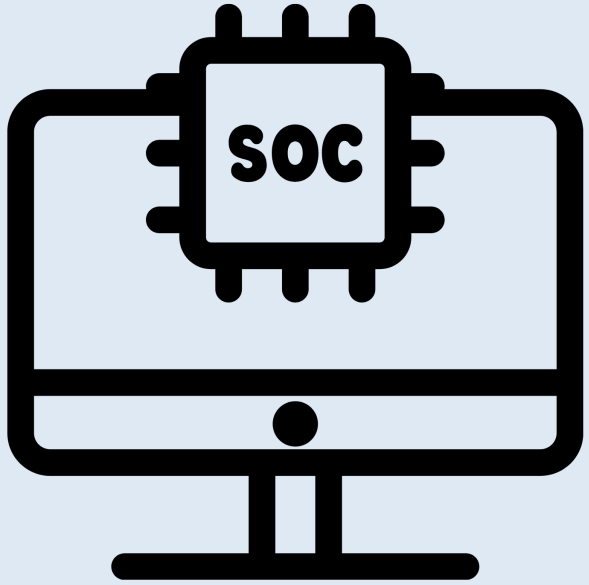
3.2 Onboarding

3.3 Fullmakt

3.4 Sikkerhetspakker for programvare

3.5 Prioritering av alarmer

3.6 Håndtere alarmer



# Anbefalinger

## 3. Ansvarsfordeling

3.1  SOC leverer tjenesten

3.2 Onboarding

**3.3 Fullmakt**

3.4 Sikkerhetspakker for programvare

3.5 Prioritering av alarmer

3.6 Håndtere alarmer

# Anbefalinger

## 3. Ansvarsfordeling

3.1 SOC leverer tjenesten

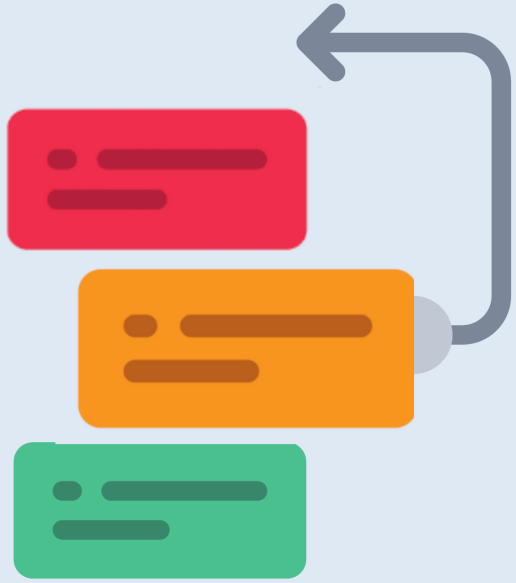
3.2 Onboarding

3.3 Fullmakt

3.4 Sikkerhetspakker for programvare

**3.5 Prioritering av alarmer**

3.6 Håndtere alarmer



# Anbefalinger

## 4. Kompetanse en kommune bør ha

4.1 Styrende dokumenter for informasjonssikkerhet

**4.2 ISAC medlemskap**

4.3 Datahåndtering

4.4 Involvere alle ledd i sikkerhetskulturen

4.5 Skaffe sikkerhetskompetanse

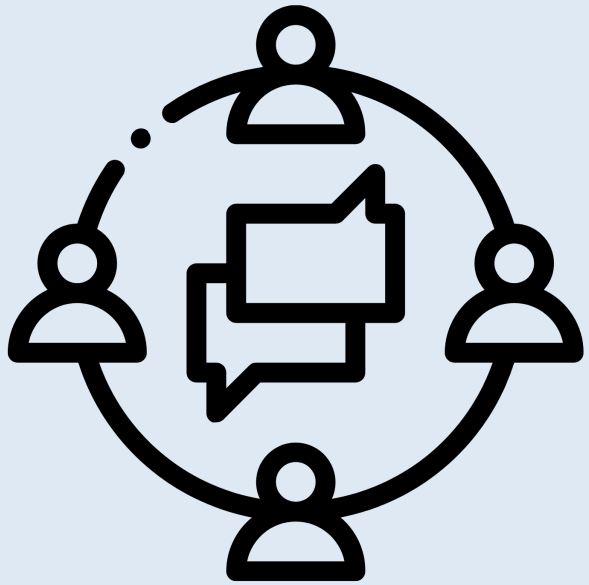
4.6 Prosjektstyring

4.7 Relevant erfaring eller utdanning

4.8 Rekruttering og synlighet

4.9 Obligatoriske og periodiske sikkerhetskurs

4.10 Egne forum eller kanaler for sikkerhets relaterte temaer



# Anbefalinger

## 4. Kompetanse en kommune bør ha

4.1 Styrende dokumenter for informasjonssikkerhet

4.2 ISAC medlemskap

4.3 Datahåndtering

4.4 Involvere alle ledd i sikkerhetskulturen

**4.5 Skaffe sikkerhetskompetanse**

4.6 Prosjektstyring

4.7 Relevant erfaring eller utdanning

4.8 Rekruttering og synlighet

4.9 Obligatoriske og periodiske sikkerhetskurs

4.10 Egne forum eller kanaler for sikkerhets relaterte temaer

# Anbefalinger

## 4. Kompetanse en kommune bør ha

4.1 Styrende dokumenter for informasjonssikkerhet

4.2 ISAC medlemskap

4.3 Datahåndtering

4.4 Involvere alle ledd i sikkerhetskulturen

4.5 Skaffe sikkerhetskompetanse

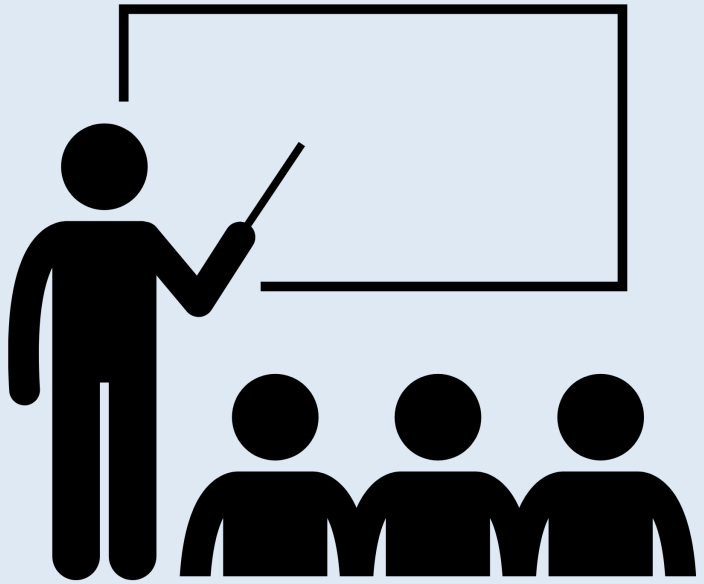
4.6 Prosjektstyring

4.7 Relevant erfaring eller utdanning

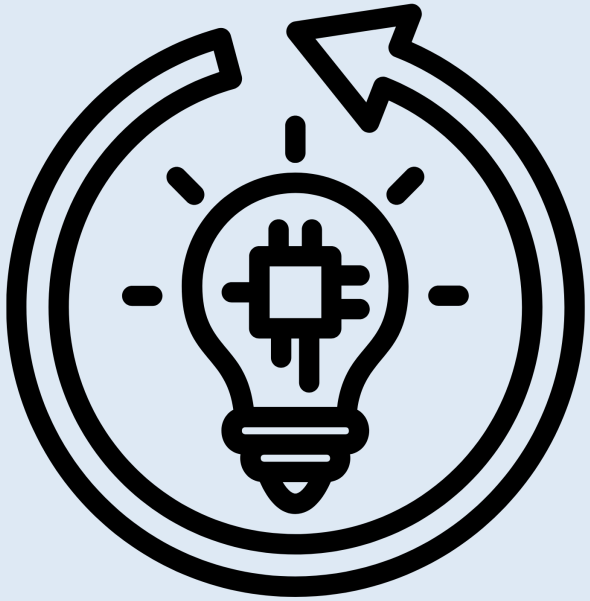
4.8 Rekruttering og synlighet

**4.9 Obligatoriske og periodiske sikkerhetskurs**

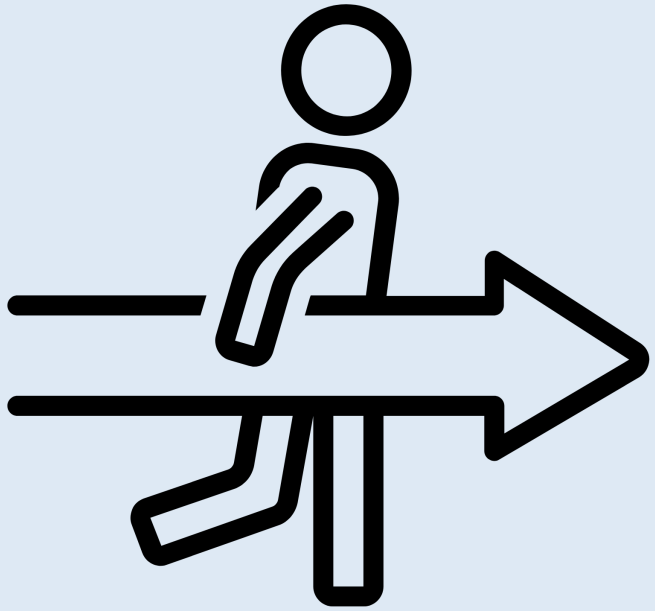
4.10 Egne forum eller kanaler for sikkerhets relaterte temaer



# Avslutning



## Konklusjon



## Videre arbeid

- SOC kompetanse
- Intern SOC
- Felles SOC

# TAKK FOR OSS