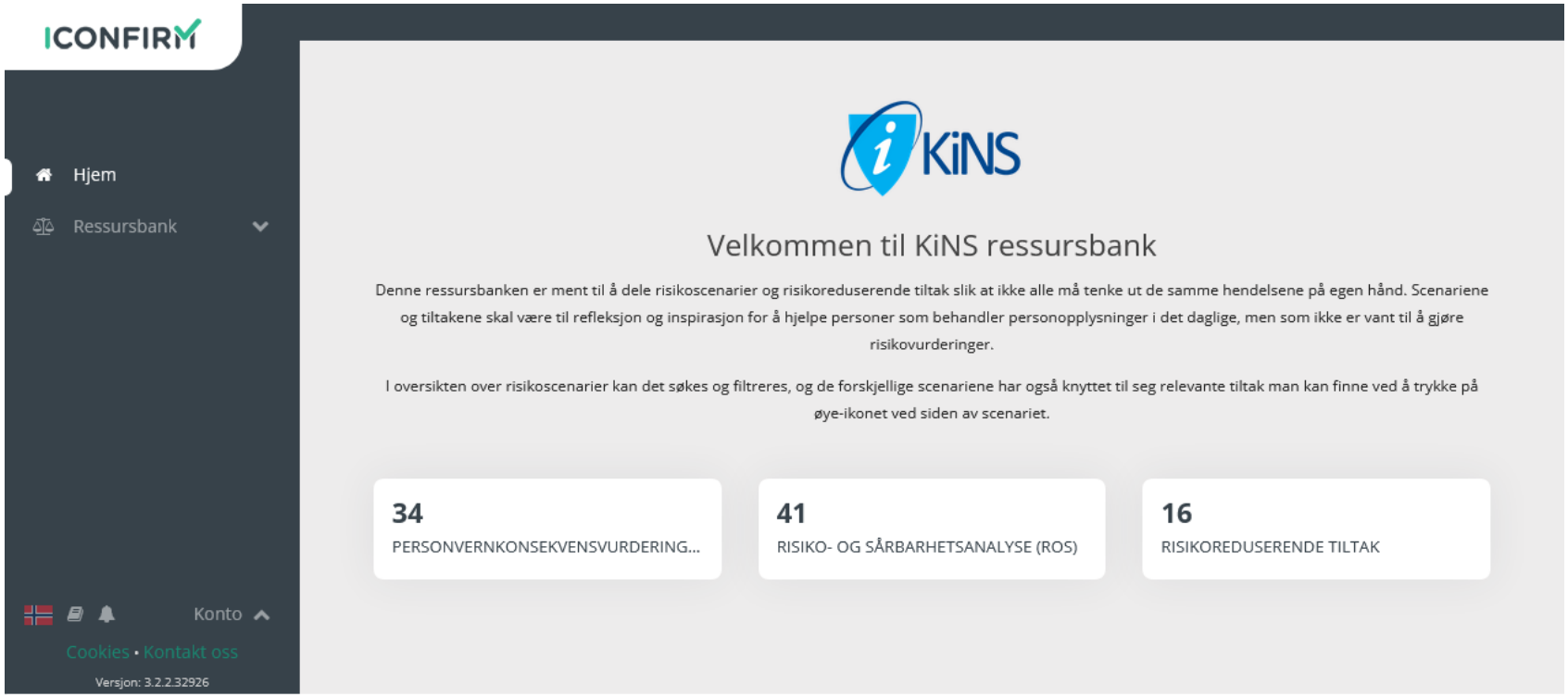
KiNS
foreningen kommunal informasjonssikkerhet

Ressursbank for risiko og tiltak

21. April 2022

Framside


ICONFIRM
Hjem
Ressursbank
Konto
Cookies • Kontakt oss
Versjon: 3.2.2.32926
KiNS
Velkommen til KiNS ressursbank
Denne ressursbanken er ment til å dele risikoscenarier og risikoreduserende tiltak slik at ikke alle må tenke ut de samme hendelsene på egen hånd. Scenariene og tiltakene skal være til refleksjon og inspirasjon for å hjelpe personer som behandler personopplysninger i det daglige, men som ikke er vant til å gjøre risikovurderinger.
I oversikten over risikoscenarier kan det søkes og filtreres, og de forskjellige scenariene har også knyttet til seg relevante tiltak man kan finne ved å trykke på øye-ikonet ved siden av scenariet.
34
PERSONVERNKONSEKVENSVURDERING...
41
RISIKO- OG SÅRBARHETSANALYSE (ROS)
16
RISIKOREDUSERENDE TILTAK

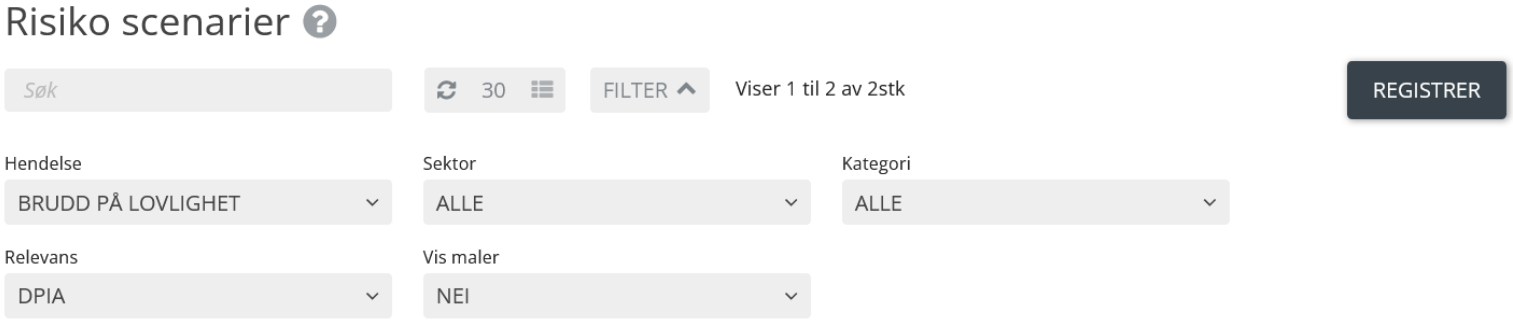
Risikoscenarier

Risiko scenarier

Søk | 30 | FILTER | Viser 1 til 30 av 41stk | REGISTRER

HENDELSE	ÅRSAK	BESKRIVELSE	VALG
Beskyttelsesverdige opplysninger blir tilgjengelig for uvedkommende	Passord på avveie	Ansatte deler med andre (feks barn). Uvedkommende får tak i ansattes passord.	
Svindel og ID-tyveri			

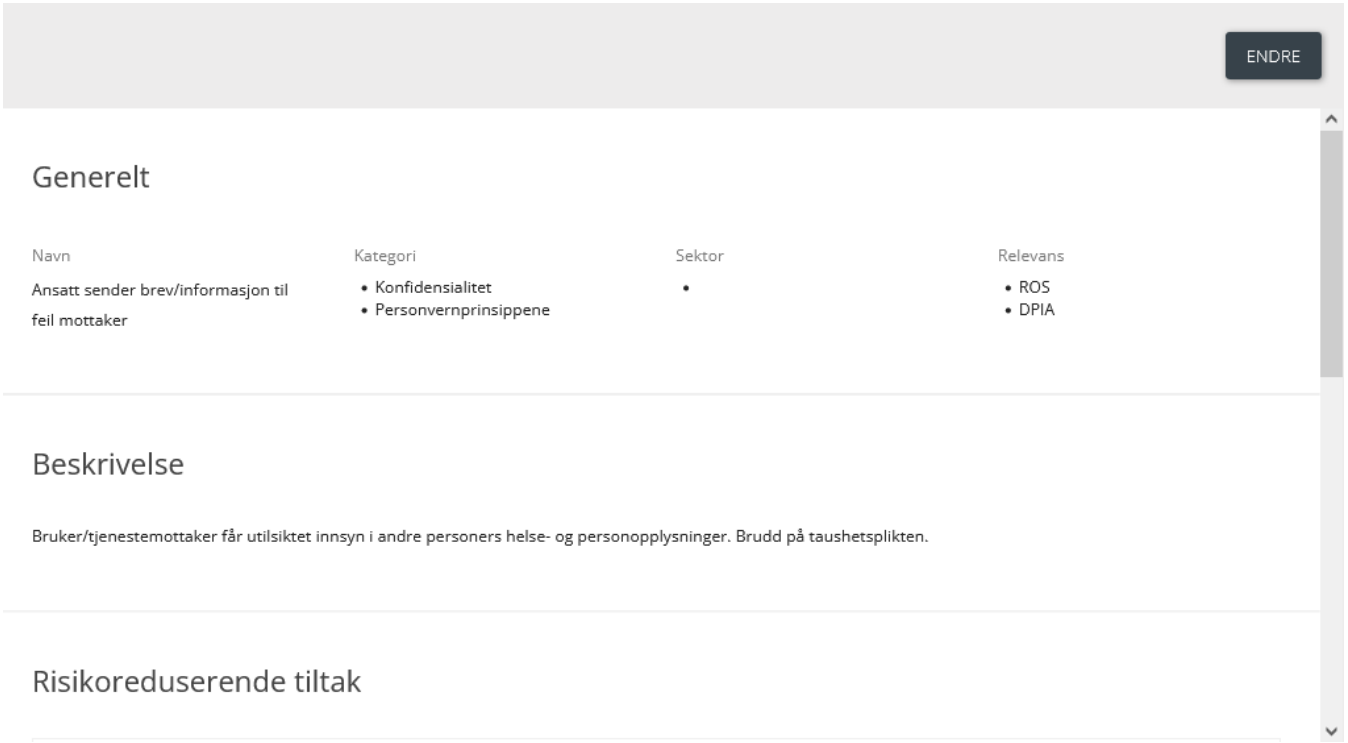
Filtrering


Risiko scenarier
Søk
30
FILTER
Viser 1 til 2 av 2stk
REGISTRER
Hendelse
BRUDD PÅ LOVLIGHET
Sektor
ALLE
Kategori
ALLE
Relevans
DPIA
Vis maler
NEI

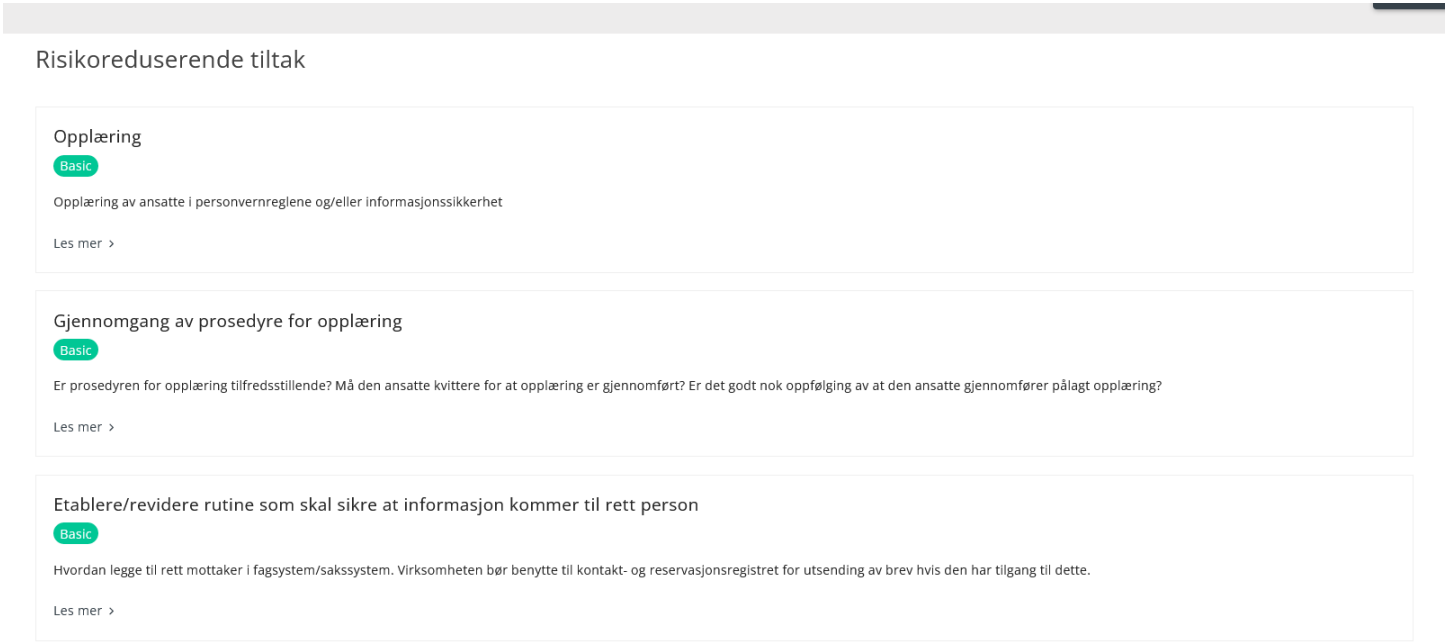
Eksempel nr. 1

Opplysninger blir tilgjengelig for uvedkommende Brudd på lovlighet Brudd på ansvarlighet	Ansatt sender brev/informasjon til feil mottaker	Bruker/tjenestemottaker får utilsiktet innsyn i andre personers helse- og personopplysninger. Brudd på taushetsplikten.	 

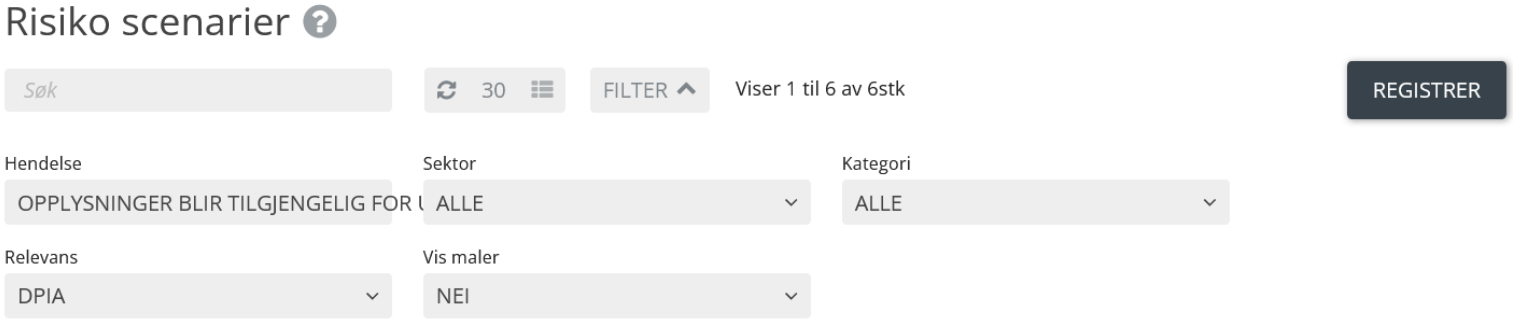
Eksempel nr. 1



Eksempel nr. 1 - tiltak



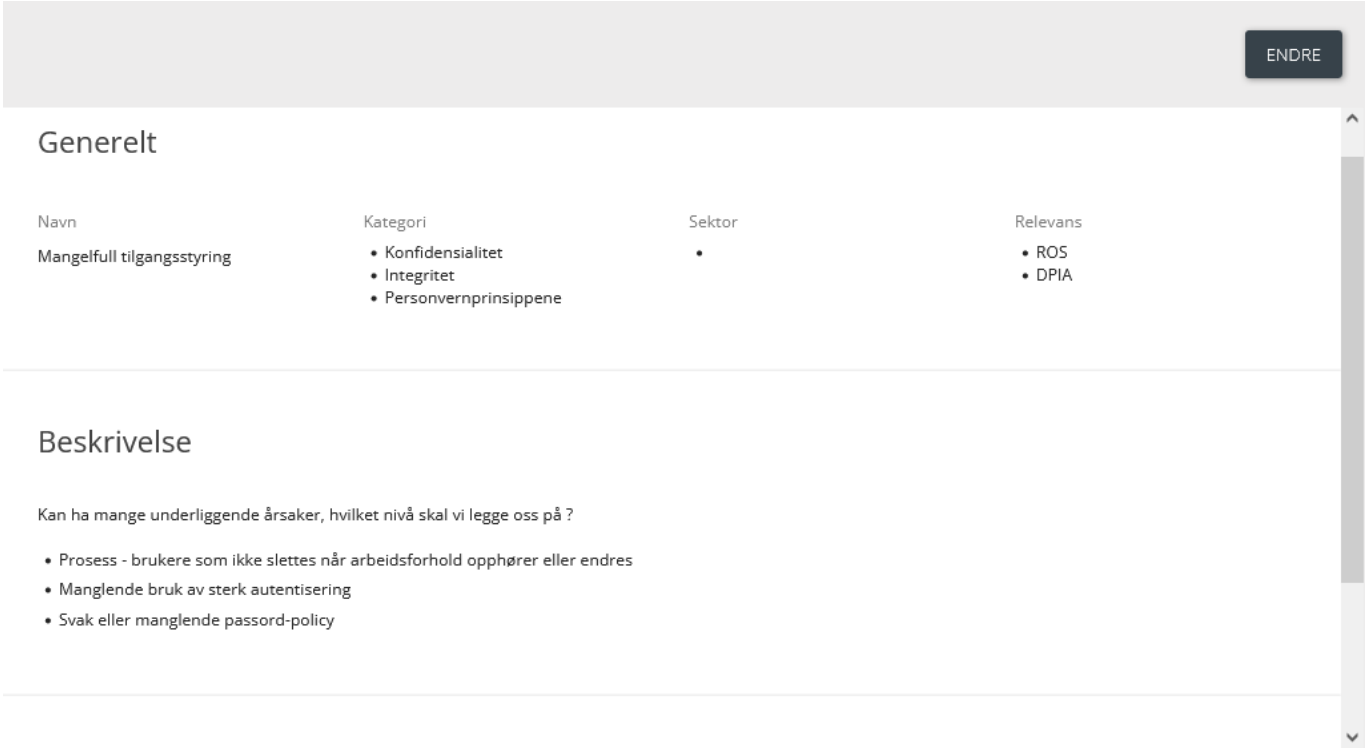
Filtrering nr. 2



Eksempel nr. 2

Opplysninger blir tilgjengelig for uvedkommende Ødeleggelse av data Tap av data Snoking og misbruk av tilgang til informasjon Brudd på ansvarlighet	Mangelfull tilgangsstyring	Kan ha mange underliggende årsaker, hvilket nivå skal vi legge oss på ?Prosess - brukere som ikke slettes når arbeidsforhold opphører eller endresManglende bruk av sterk autentiseringSvak eller manglende passord-policy	 

Eksempel nr. 2



Eksempel nr. 2 - tiltak

Risikoreduserende tiltak

Krav om sterk autentisering (MFA)

Professional

Les mer ›

NSM 2.6.2 - Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter

Basic

Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter. a) Prosessen bør omhandle i) kontoer til brukere, enheter og systemprosesser, ii) tilganger til systemer og applika...

Les mer ›

NSM 2.6.1 - Etabler retningslinjer for tilgangskontroll

Professional

Etabler retningslinjer for tilgangskontroll. a) Retningslinjene bør dekke flest mulig av ressursene i virksomheten: brukere, klienter, felles-mapper, server-applikasjoner, servere, nettverksenheter, ...

Les mer ›

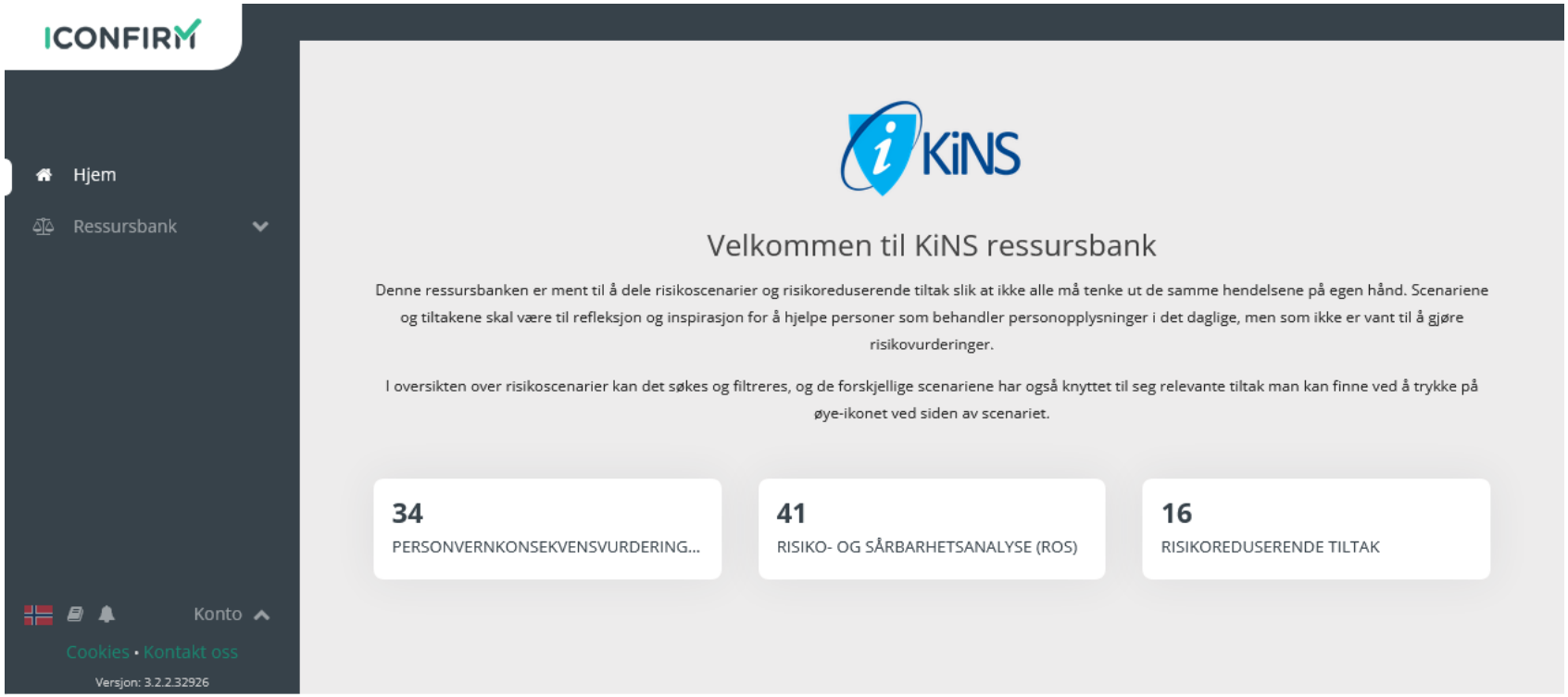
NSM 2.6.3 - Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter

Professional

Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter. a) Styr kontoer, tilganger og rettigheter til flest mulig av ressurser (ref. 2.6.2.a) i virksomheten m...

Les mer ›

Framside


ICONFIRM
Hjem
Ressursbank
Konto
Cookies • Kontakt oss
Versjon: 3.2.2.32926
KiNS
Velkommen til KiNS ressursbank
Denne ressursbanken er ment til å dele risikoscenarier og risikoreduserende tiltak slik at ikke alle må tenke ut de samme hendelsene på egen hånd. Scenariene og tiltakene skal være til refleksjon og inspirasjon for å hjelpe personer som behandler personopplysninger i det daglige, men som ikke er vant til å gjøre risikovurderinger.
I oversikten over risikoscenarier kan det søkes og filtreres, og de forskjellige scenariene har også knyttet til seg relevante tiltak man kan finne ved å trykke på øye-ikonet ved siden av scenariet.
34
PERSONVERNKONSEKVENSVURDERING...
41
RISIKO- OG SÅRBARHETSANALYSE (ROS)
16
RISIKOREDUSERENDE TILTAK