

# Kartlegging av høyrisikoroller

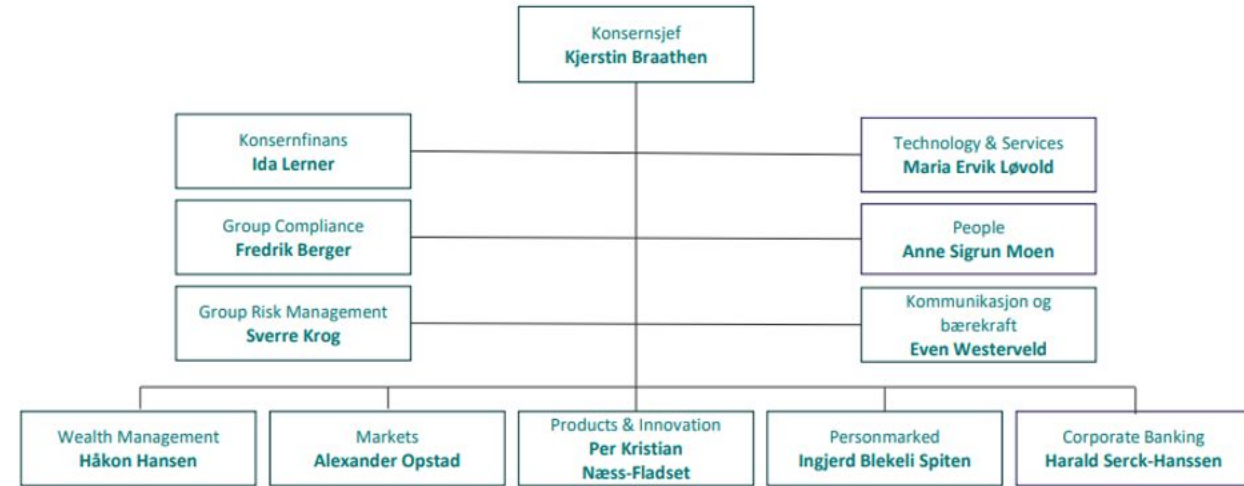
Sikkerhetsfestivalen 30. august 2023

Richard Hansen og Tonje Østgård

Physical- and Personnel security


Group Security

Norges største bank  
Over 10 000 ansatte  
Til stede i 18 ulike land



# DNB

# Agenda

- Hva høyriskoroller er
  - Fordeler ved å kartlegge høyriskoroller
  - Hvordan vi har gjort det i DNB
  - Lessons learned
- 

# Hva er høyriskoroller?

En høyriskorolle forvalter eller på andre måter har tilgang til virksomhetens viktigste og mest kritiske **verdier**.

---

En høyriskorolle vil implisitt være **mer utsatt** for forsøk på kompromittering av trusselaktør(er).

---

En ansatt i høyriskorolle som begår innsideaktivitet kan påføre virksomheten **kritiske konsekvenser**.



# Hovedprinsipper for kartlegging



01

Det gjelder å komme frem til verdiene som vi har **aller størst** behov for å beskytte – heller for få enn for mange i starten

---

02

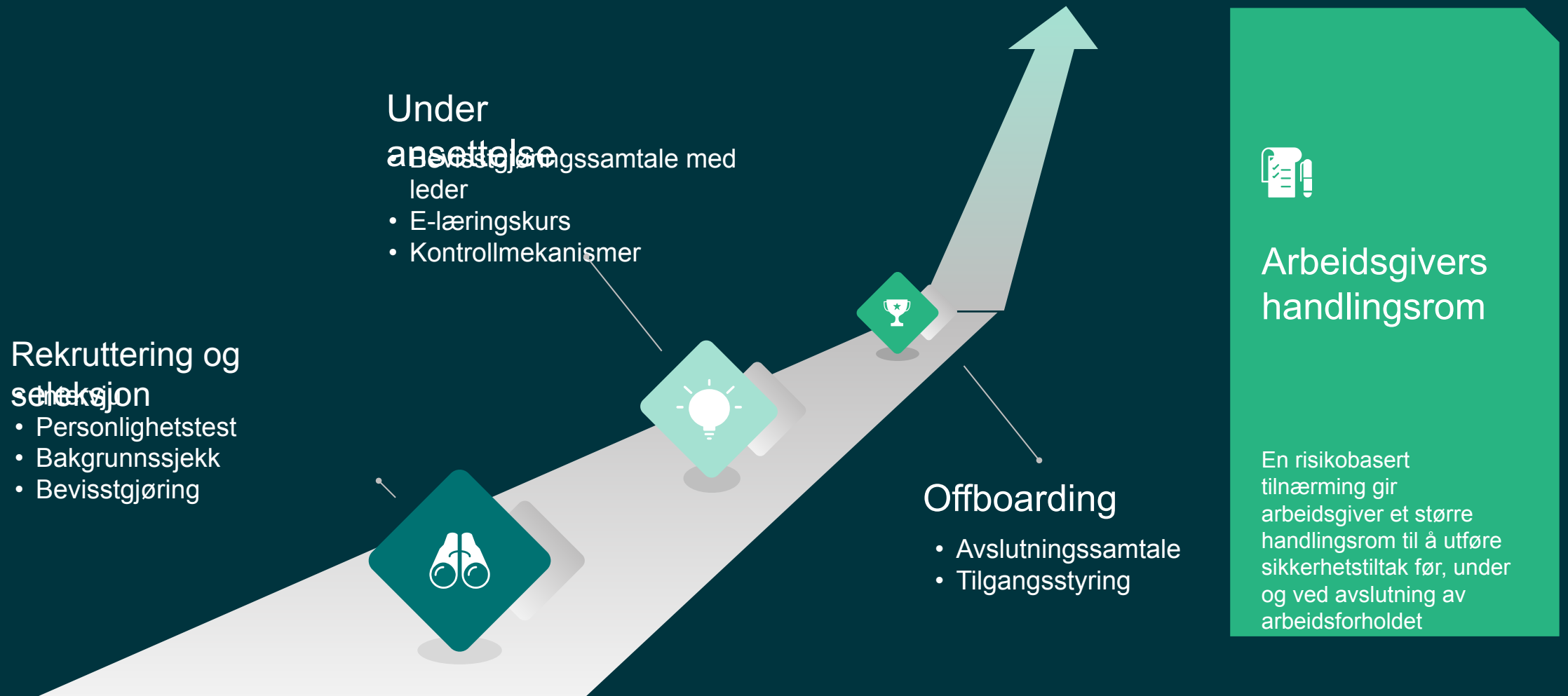
Kartleggingen skal være **kontekst spesifikk** og tilpasset forretnings- eller støtteområdet. Områdene kjenner sine roller best, men Group Security bistår.

---

03

Kartleggingen skal være en **objektiv vurdering** av risiko knyttet til rollen. Under kartleggingen skal rollen vurderes på generell basis og ikke sett opp mot personer som innehar rollen i dag.

# Hvorfor høyriskoroller?

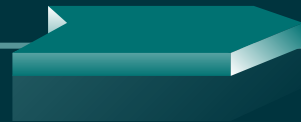


# Proseszen



## Koordinering

Det utnevnes  
kartleggingsansvarlig(  
.e) i avdelingen



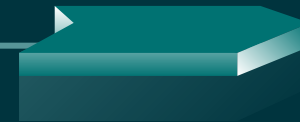
## Rådgivning

Sikkerhetsavdelingen  
bistår med rådgivning  
.og workshops



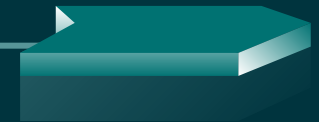
## Godkjenning

Resultatet  
godkjennes på angitt  
.ledernivå



## HR-system

En oversikt over ansatte i  
høyrisikroller føres inn i  
.HR-systemet



## Tiltak

Det implementeres  
tiltak for ansatte som  
innehar eller skal  
inneha en  
.høyrisikrolle

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarioer</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>



# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarioer</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder					
Fagleder					
Fagspesialist					
Koordinator					
Lærling					

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarioer</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li><li>• Beslutningsmyndighet</li></ul>				
Fagleder	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li><li>• Administrative rettigheter</li></ul>				
Fagspesialist	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li></ul>				
Koordinator	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li></ul>				
Lærling	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li></ul>				

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarier</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li><li>• Beslutningsmyndighet</li></ul>	<ul style="list-style-type: none"><li>• Seksjonsleder lekker informasjon om sikkerhetstiltak</li><li>• Seksjonsleder gir trusselaktører adgang til kritisk infrastruktur</li><li>• Seksjonsleder tar beslutninger til skade for bedriften</li></ul>			
Fagleder	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li><li>• Administrative rettigheter</li></ul>	<ul style="list-style-type: none"><li>• Fagleder lekker informasjon om sikkerhetstiltak</li><li>• Fagleder gir trusselaktører adgang til kritisk infrastruktur</li><li>• Fagleder utnytter sine utvidede tilganger for å påvirke funksjonaliteten i kritiske systemer</li></ul>			
Fagspesialist	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li><li>• Tilgang til kritisk infrastruktur</li></ul>	<ul style="list-style-type: none"><li>• Fagspesialist lekker informasjon om sikkerhetstiltak</li><li>• Fagspesialist gir trusselaktører adgang til kritisk infrastruktur</li></ul>			
Koordinator	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li></ul>	<ul style="list-style-type: none"><li>• Koordinator lekker informasjon om sikkerhetstiltak</li></ul>			
Lærling	<ul style="list-style-type: none"><li>• Kunnskap om sikkerhetstiltak</li></ul>	<ul style="list-style-type: none"><li>• Lærling lekker informasjon om sikkerhetstiltak</li></ul>			

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarier</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Beslutningsmyndighet</li> </ul>	<ul style="list-style-type: none"> <li>• Seksjonsleder lekker informasjon om sikkerhetstiltak</li> <li>• Seksjonsleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Seksjonsleder tar beslutninger til skade for bedriften</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>		
Fagleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Administrative rettigheter</li> </ul>	<ul style="list-style-type: none"> <li>• Fagleder lekker informasjon om sikkerhetstiltak</li> <li>• Fagleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Fagleder utnytter sine utvidede tilganger for å påvirke funksjonaliteten i kritiske systemer</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• En eller flere kritiske tjenester settes ut av spill</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>		
Fagspesialist	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Fagspesialist lekker informasjon om sikkerhetstiltak</li> <li>• Fagspesialist gir trusselaktører adgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>		
Koordinator	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Koordinator lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>		
Lærling	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Lærling lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>		

# Konsekvensmatrise

Konsekvens	Ubetydelig	Moderat	Alvorlig	Kritisk
Compliance	Tilsyn uten særskilte merknader	Tilsyn med merknader	Pålegg fra tilsynsmyndighet, og/eller bøter	Tap av konsesjoner
Omdømme	Negativ enkeltoppslag (dag/dager)	Begrenset negativ medieomtale (dager)	Negativ medieomtale (uker)	Negativ medieomtale (måneder)
Drift	Mindre forstyrrelser knyttet til driften.	Driften er oppe og går, men med redusert kvalitet.	Driften er så vidt oppe og går, med svært redusert kvalitet.	En eller flere kritiske tjenester er satt helt ut av spill.
Økonomi	Tap av inntekter/økte kostnader opp til \$ NOK	Tap av inntekter/økte kostnader for \$\$ NOK	Tap av inntekter/økte kostnader for \$\$\$ NOK	Tap av inntekter/økte kostnader som overstiger \$\$\$\$ NOK

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarier</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Beslutningsmyndighet</li> </ul>	<ul style="list-style-type: none"> <li>• Seksjonsleder lekker informasjon om sikkerhetstiltak</li> <li>• Seksjonsleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Seksjonsleder tar beslutninger til skade for bedriften</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Alvorlig	
Fagleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Administrative rettigheter</li> </ul>	<ul style="list-style-type: none"> <li>• Fagleder lekker informasjon om sikkerhetstiltak</li> <li>• Fagleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Fagleder utnytter sine utvidede tilganger for å påvirke funksjonaliteten i kritiske systemer</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• En eller flere kritiske tjenester settes ut av spill</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Kritisk	
Fagspesialist	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Fagspesialist lekker informasjon om sikkerhetstiltak</li> <li>• Fagspesialist gir trusselaktører adgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Alvorlig	
Koordinator	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Koordinator lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	
Lærling	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Lærling lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarier</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Beslutningsmyndighet</li> </ul>	<ul style="list-style-type: none"> <li>• Seksjonsleder lekker informasjon om sikkerhetstiltak</li> <li>• Seksjonsleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Seksjonsleder tar beslutninger til skade for bedriften</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Alvorlig	Nei
Fagleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Administrative rettigheter</li> </ul>	<ul style="list-style-type: none"> <li>• Fagleder lekker informasjon om sikkerhetstiltak</li> <li>• Fagleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Fagleder utnytter sine utvidede tilganger for å påvirke funksjonaliteten i kritiske systemer</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• En eller flere kritiske tjenester settes ut av spill</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Kritisk	Ja
Fagspesialist	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Fagspesialist lekker informasjon om sikkerhetstiltak</li> <li>• Fagspesialist gir trusselaktører adgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Alvorlig	Nei
Koordinator	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Koordinator lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	Nei
Lærling	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Lærling lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	Nei

# Kartleggingsmatrisen

<i>Rollenavn</i>	<i>Kritiske verdier</i>	<i>Verstefallscenarioer</i>	<i>Mulige konsekvenser</i>	<i>Høyeste konsekvens</i>	<i>Høyrisikorolle ?</i>
Seksjonsleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Beslutningsmyndighet</li> </ul>	<ul style="list-style-type: none"> <li>• Seksjonsleder lekker informasjon om sikkerhetstiltak</li> <li>• Seksjonsleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Seksjonsleder tar beslutninger til skade for bedriften</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Alvorlig	Nei
Fagleder	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> <li>• Administrative rettigheter</li> </ul>	<ul style="list-style-type: none"> <li>• Fagleder lekker informasjon om sikkerhetstiltak</li> <li>• Fagleder gir trusselaktører adgang til kritisk infrastruktur</li> <li>• Fagleder utnytter sine utvidede tilganger for å påvirke funksjonaliteten i kritiske systemer</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• En eller flere kritiske tjenester settes ut av spill</li> <li>• Finansielle tap under NOK \$\$\$</li> </ul>	Kritisk	Ja
Fagspesialist	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> <li>• Tilgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Fagspesialist lekker informasjon om sikkerhetstiltak</li> <li>• Fagspesialist gir trusselaktører adgang til kritisk infrastruktur</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en eller flere dager)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Alvorlig	Nei
Koordinator	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Koordinator lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	Nei
Lærling	<ul style="list-style-type: none"> <li>• Kunnskap om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Lærling lekker informasjon om sikkerhetstiltak</li> </ul>	<ul style="list-style-type: none"> <li>• Medieoppslag (en dag)</li> <li>• Betydelige reaksjoner fra myndigheter</li> <li>• Mindre forstyrrelser knyttet til drift</li> <li>• Finansielle tap under NOK \$\$</li> </ul>	Moderat	Nei



# Lessons learned

- ✓ Benytt tidligere risikovurderinger
- ✓ Ta utgangspunkt i systemene når dere kartlegger IT-ansatte
- ✓ Identifiser heller for få enn for mange i starten
- ✓ Opplever at ofte har man svært mange eller ingen høyrisikoroller
- ✓ Ha tiltakene klare før dere setter i gang med kartleggingen



# Tilbakemeldinger

- «Bra at man får fokus på risikoroller og sårbarheter.»
- «Bra at dette temaet kommer i et kurs. Tror det er nyttig for mange medarbeidere som sitter i høyrisikoroller.»
- «Bevisstgjøring for alle.»
- «Påminnelse og informasjon om støtte fra arbeidsgiver ved behov.»
- «En viktig påminnelse om hvor bevisste vi må være i forhold til jobben vi har og hva vi kan bli utsatt for.»



[Dette bildet](#) av Ukjent forfatter er lisensiert under [CC BY-SA](#)



# Spørsmål eller innspill?

Ta gjerne kontakt med oss!

Tonje Østgård: [tonje.ostgard@dnb.no](mailto:tonje.ostgard@dnb.no)

Tlf. 91 52 13 12

Richard Hansen: [richard.hansen@dnb.no](mailto:richard.hansen@dnb.no)

Tlf. 41 68 57 25