



## Risikostyring – på den fede måde!

v/Anahita Khatam-Lashgari  
Chefkonsulent, databeskyttelsesagent, teamkoordinator for Risikostyring

# Agenda

- Risiko(vurdering) – hvad er det?
- Hvordan har SDS gjort det nemmere at involvere forretningen?
- Hvor hurtigt kan en risikovurdering gennemføres?
- Hvad skal man gøre ekstra, når NIS2 skal efterleves?
- Perspektivering

# Risiko(vurdering) – hvad er det?

- Projekt risiko
- Økonomisk risiko
  
- Informationssikkerheds risiko
- GDPR risiko
- NIS risiko

# Risiko(vurdering) – hvad er det? – fortsat

Sårbarhed



Trussel



Sandsynlighed

Konsekvens

Risiko

## **FIT(A)**

- Fortrolighed
- Integritet
- Tilgængelighed
- (Autenticitet)

# Risiko(vurdering) – hvad er det? – fortsat

## Udfordring:

- Når man skal igennem et håndværk, som ikke har en facitliste, hvordan involveres forretningen bedst?
- Hvordan får man sin forretning til at forstå konsekvens og sandsynlighed?

# Hvordan har SDS gjort det nemmere at involvere forretningen?

**KONSEKVENSS**  
**FORTROLIGHED**

Ved vurderingen af 'fortrolighed' forstås konsekvensen af, at de personoplysninger, der behandles, kommer uberettigede til kendskab. Konsekvensen af dette skal indgå i risikovurderingen.

Hvilken konsekvens vurderes der for den registrerede at være forbundet med brud på fortrolighed?

Vælg:

Meget lav

Lav

Mellem

Høj

Meget høj

Begrund dette svar (Begynd med stort begyndelsesbogstav og slut med punktum)

## NETVÆRK OG TEKNISKE BEHANDLINGSMIDLER

Sker dele af behandlingen af personoplysninger gennem det åbne internet, eller er det i øvrigt muligt at tilgå systemet gennem det åbne internet?

- Ja
- Nej

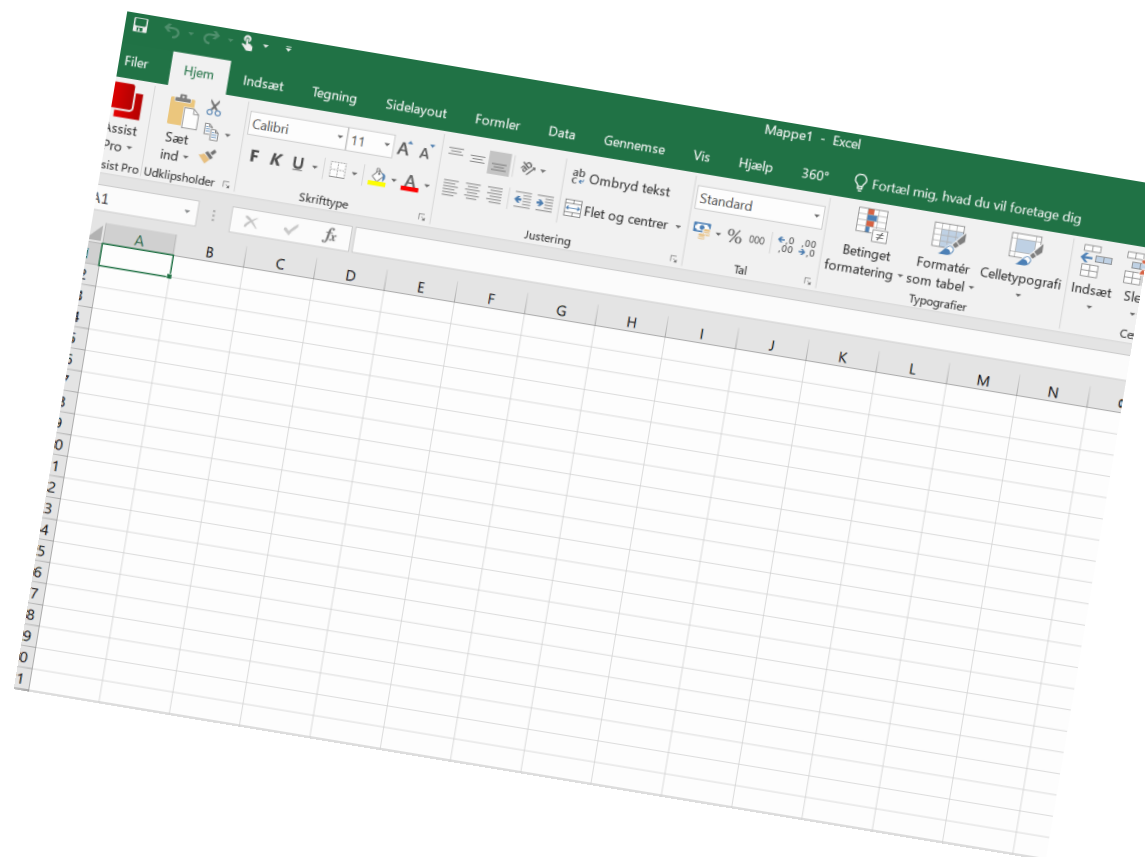
Indsæt evt. kommentar til den pågældende sårbarhed

Angiv, hvilke(n) trusler/trussel der er tilknyttet denne sårbarhed (Begynd med stort begyndelsesbogstav og slut med punktum). (Kan der ikke identificeres nogen trusler, angives f.eks. "Ingen kendte trusler")

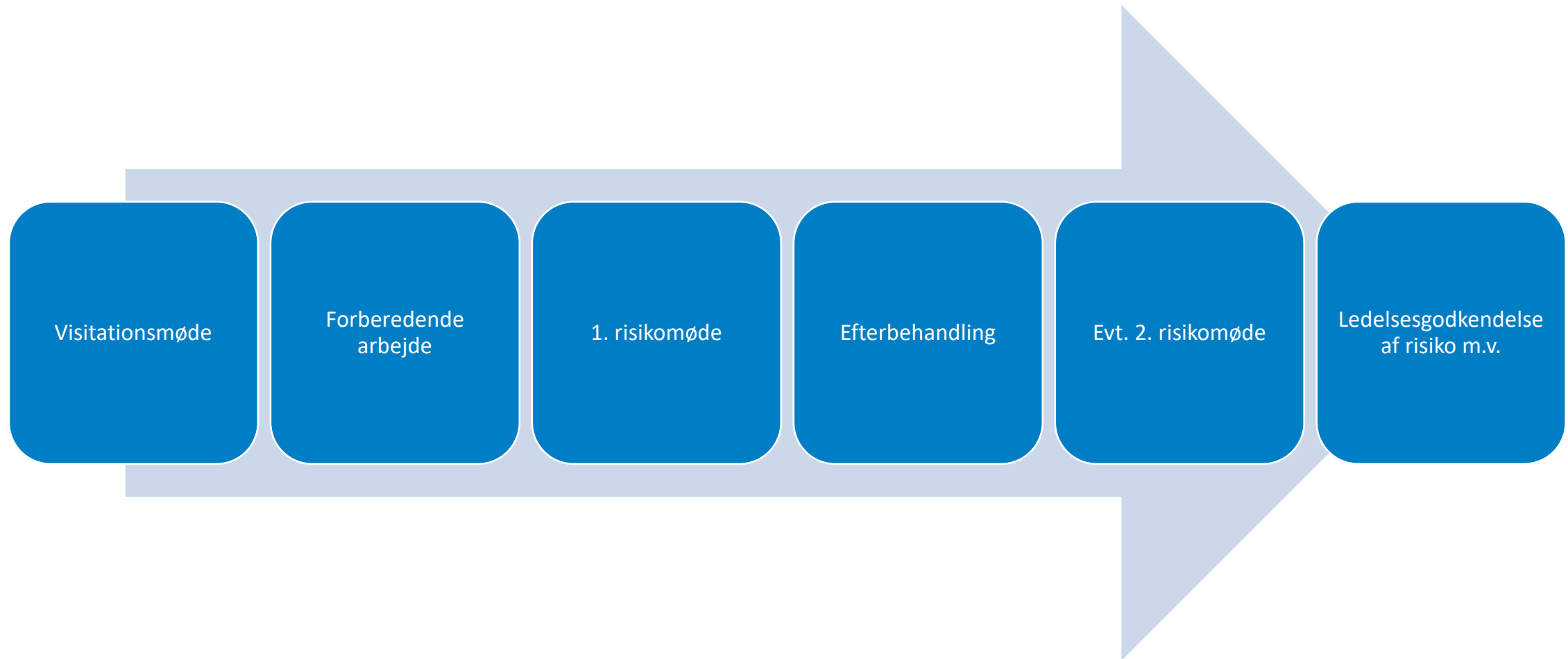
Angiv de(n) mitigerende foranstaltning(er), der nedbringer sandsynligheden for, at den identificerede trussel realiseres (Begynd med stort begyndelsesbogstav og slut med punktum). (Kan der ikke identificeres mitigerende foranstaltninger, angives f.eks. "Ingen mitigerende foranstaltning identificeret").

Er det muligt at tildele adgang til et system, hvor der behandles personoplysninger, gennem internettet? (fx for udvalgte brugere eller brugergrupper)?

- Ja
- Nej



# Hvordan har SDS gjort det nemmere at involvere forretningen?



# Hvor hurtigt kan en risikovurdering gennemføres?

- Hvad er omfanget af det, der skal risikovurderes?
- Er dem, der skal have lavet risikovurderingen, nye i gamet?
  - Kan de evt. selv lave det?
- Har man lavet en tidligere lignende risikovurdering?
- Hvor tæt på 100% vil man være ift. sin risikovurdering?
- Er det en genbesøg af risikovurdering?



# Hvad skal man gøre ekstra, når NIS2 skal efterleves?

- Er ens område/forretning omfattet af NIS2?
- Konsekvensdel
  - Samfundet
- Autenticitet
  
- ... Vi arbejder på at integrere i vores risikovurderinger 😊

# Perspektivering

- Tema for eSundhed: *”Sundhedsvæsenets digitale fordør – hvilke muligheder åbner den op for?”*
  - Der et ønske om at flytte patientbehandlingen hjem til borgeren med f.eks. digitale løsninger
- Patientsikkerheden skal også sikres med risikovurderinger
  - Konsekvensen af at overlade mere og mere behandling hos patienten skal vurderes
  - Sandsynlighed for at det sætte patientsikkerheden i fare skal vurderes
- Jo mere modne Sundhedsdatastyrelsen bliver ift. risikovurdering, desto bedre patientsikkerhed sikres der

# Spørgsmål?

Tak for i dag 😊



## SUNDHEDSDATA- STYRELSEN

Sundhedsdatastyrelsen  
Ørestads Boulevard 5  
2300 København S

T: +45 7221 6800

E: [kontakt@sundhedsdata.dk](mailto:kontakt@sundhedsdata.dk)

W: [sundhedsdata.dk](http://sundhedsdata.dk)