Det tværregionale samarbejde om informationssikkerhed

Vicedirektør Carsten Lind – Region Midtjylland


GDPR


REGERINGEN
National strategi for cyber- og informationssikkerhed


NIS-direktiv


ISO 27001
verified
control
quality
approved
audit
standard
superior
company
implementing
improving
assurance
reliable
tested
information
safety
warranty
system
performance
ISMS
objective
customer target
guidance
maintaining
environment
checking
needs
principles
producing
establishing
sustainable
measuring
consumer
product
international
cost
efficiency
managing
implementation
ability
norm
certified
maintainable
standardisation
management
accredited
reliability
service confirmation
commerce
requirements
checked


USERNAME:
PASSWORD:

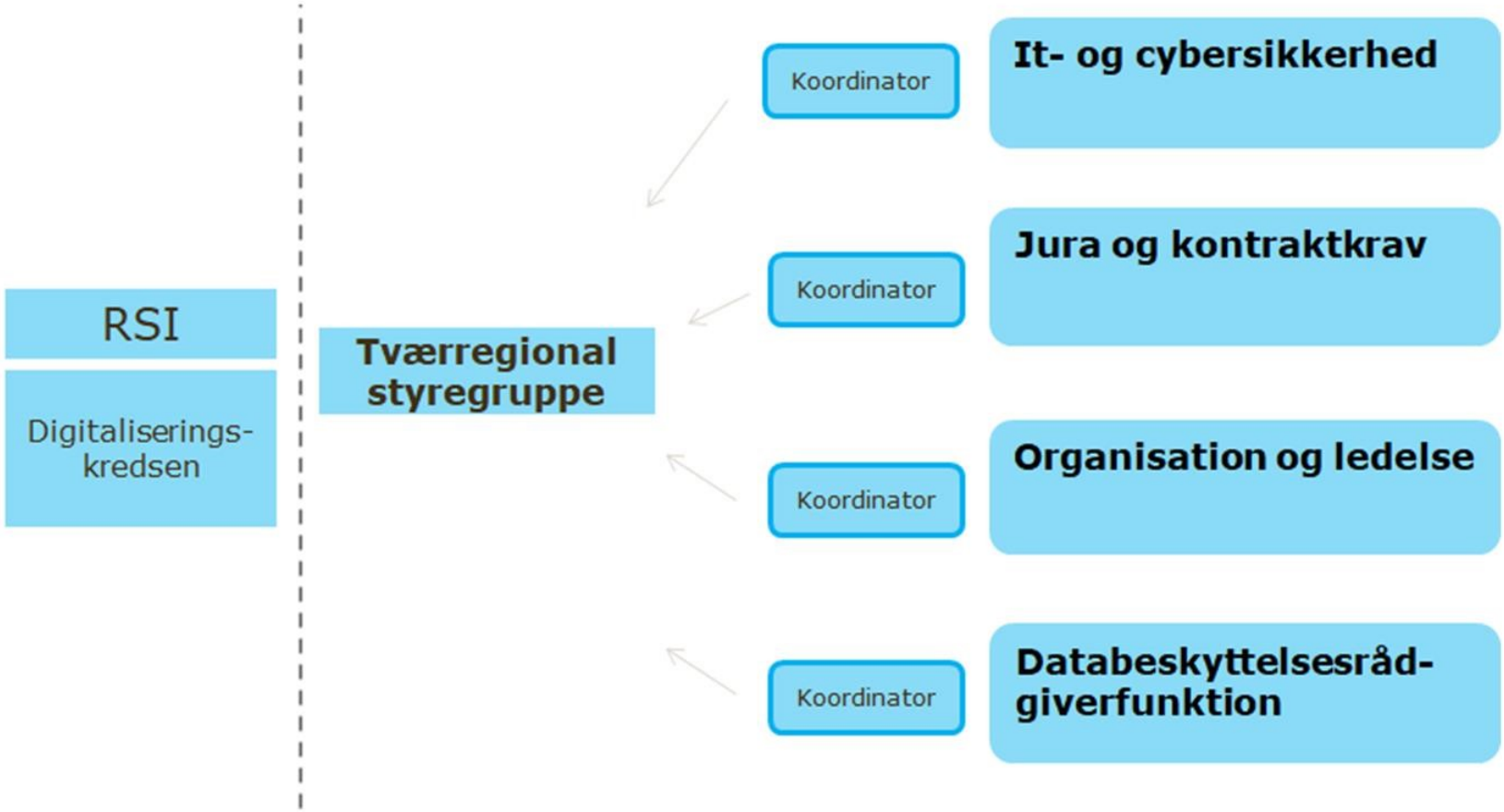

STRATEGI 2019-2022
En styrket, fælles indsats for cyber- og informationssikkerhed


ET STÆRKERE
OG MERE TRYGT
DIGITALT SAMFUND
Den fællesoffentlige digitaliseringsstrategi 2016-2020

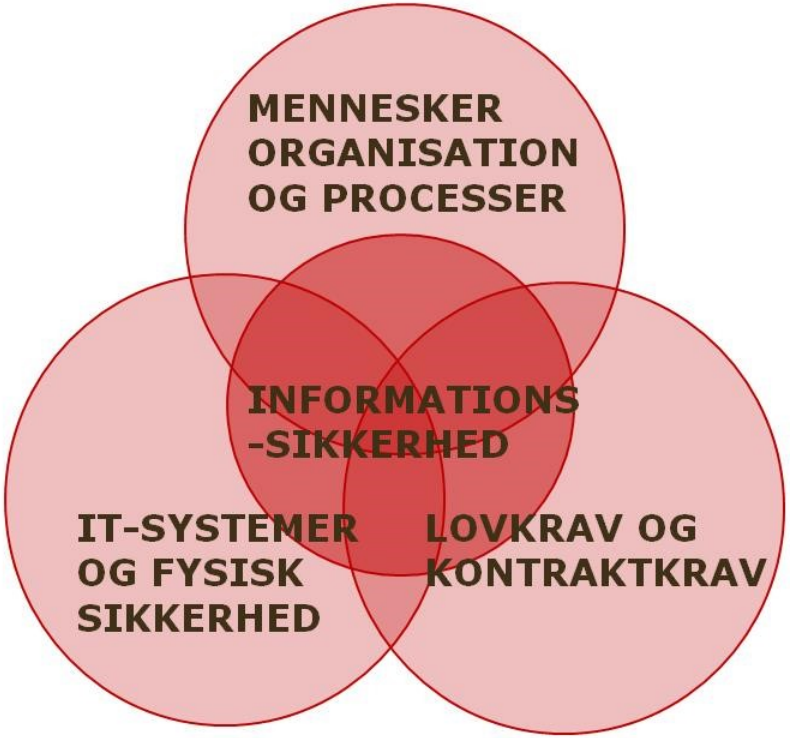
Tendenser i regionernes arbejde med informationssikkerhed

- Øget opmærksomhed og viden om informationssikkerhed blandt regionernes medarbejdere, ledelse og politikere
- Øget bevågenhed på egne styrker og sårbarheder
- Risikovurderinger
- Fokus på implementering af GDPR, ISO 27001 og strategi for cyber- og informationssikkerhed i sundhedssektoren
- Afsættelse af ressourcer i alle regioner
- Organisationsændringer – særskilte afdelinger for informationssikkerhed
- Udarbejdelse af handleplan/strategi/fokusområder

Organisering



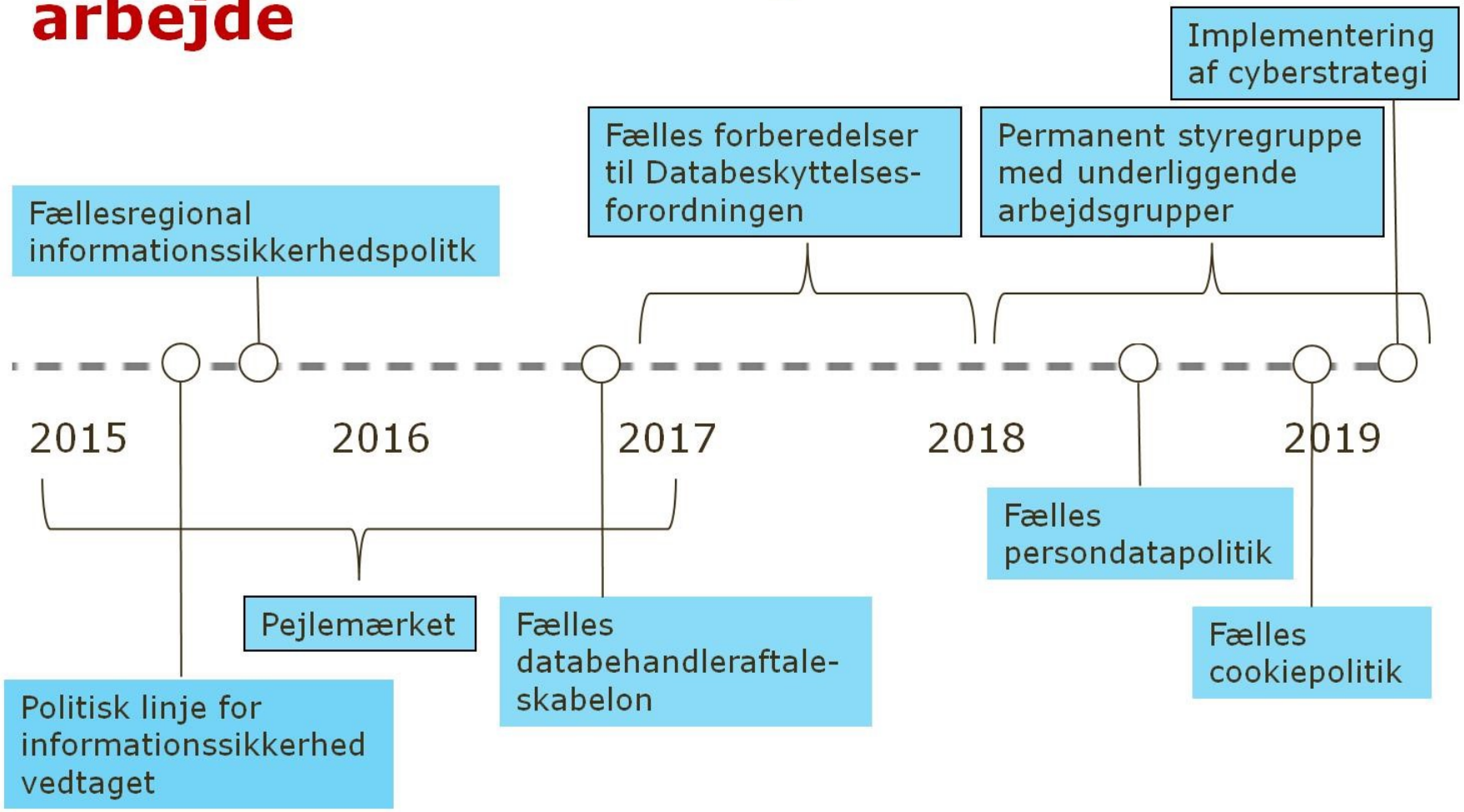
De 3 centrale elementer i informationssikkerhed



Formål med det tværregionale samarbejde

- Understøtte regionernes fælles tilgang til informationssikkerhed
- Indspil til strategiske og politisk drøftelser
- Koordinere reaktion på henvendelser fra ministerier eller medier
- Understøtte implementering af europæiske, nationale og fællesregionale initiativer, eks.:
  - Nis-direktivet
  - Den fællesoffentlige digitaliseringsstrategi 2016-2020
  - Strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022
- Bidrage til fællesregional fortolkning og forståelse af gældende lovgivning, eks.:
  - Databeskyttelsesforordningen
- Bidrage til sikkerhedsmæssig og juridisk screening af fællesregionale projekter og systemer

Tidslinje i det tværregionale arbejde



Det fællesregionale fokus

- **Fællesregionale leverancer**
  - Kontrol af databehandleraftaler
  - Fællesregional persondatapolitik
  - Fællesregional databehandleraftaleskabelon
  - Fællesregional håndtering af overførsel til tredjelande
  - Fælles skabelon for konsekvensanalyser/DPIA
  - Fællesregional Cookiepolitik
  - Minimumskrav for behandlingssikkerhed

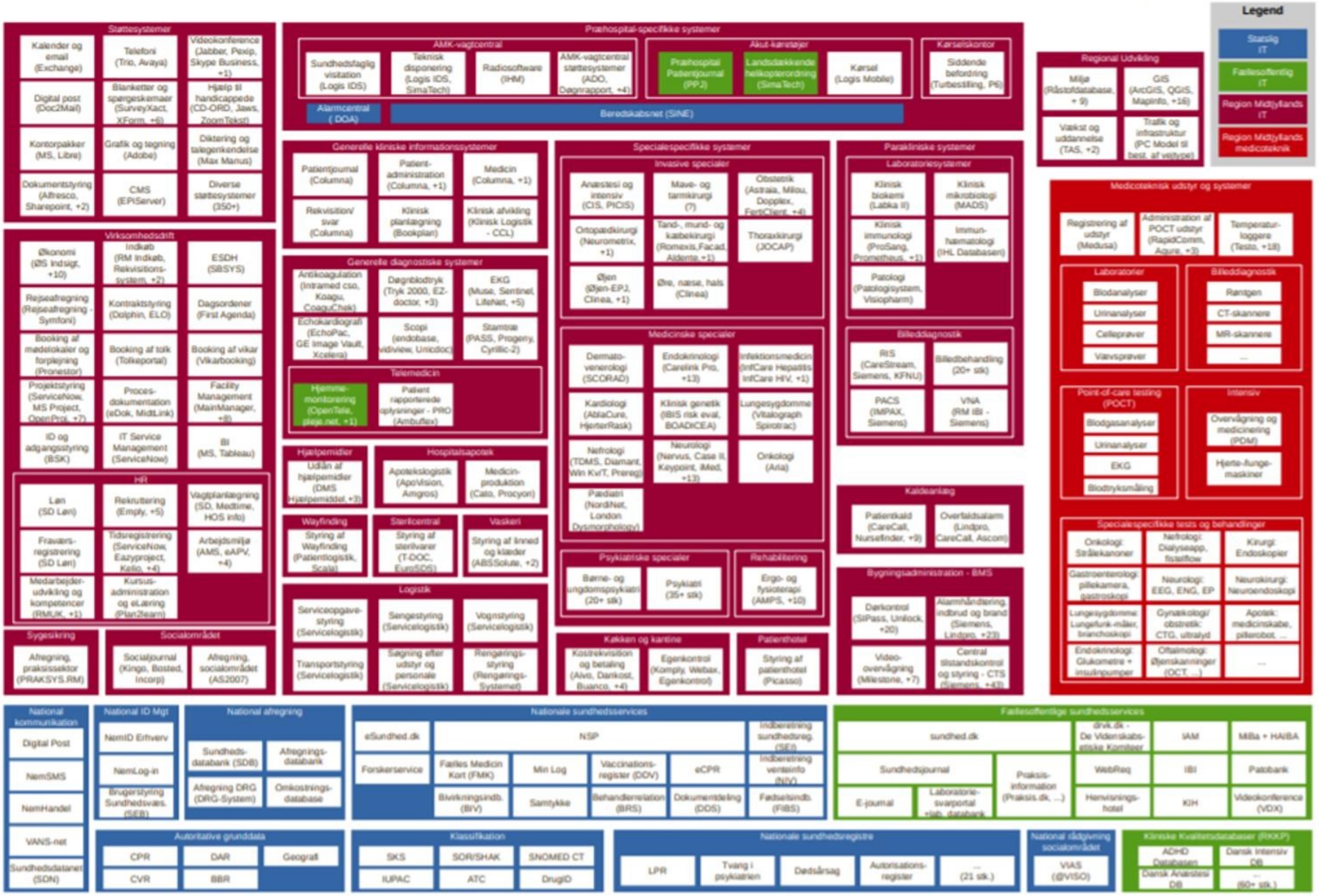
- **Fællesregional erfaringsudveksling**
  - Implementering af NIS-direktiv
  - Implementering af ISO-27001
  - Håndtering af sikkerhedsbrud
  - Log og logopfølgning
  - Awareness om informationssikkerhed
  - Slettepolitik
  - Risikovurderinger

- **Strategi for cyber-og informationssikkerhed i sundhedssektoren 2019-2022**

Udfordringer ved det tværregionale samarbejde

- Prioritering af fokusområder
- Prioritering af leverancer
- Balancen mellem fælles standard og lokal tilpasning
- Lokal forankring
- Afhængighed i forhold til lokale ressourcer
- Ledelsesmæssig opbakning

Applikationslandskab



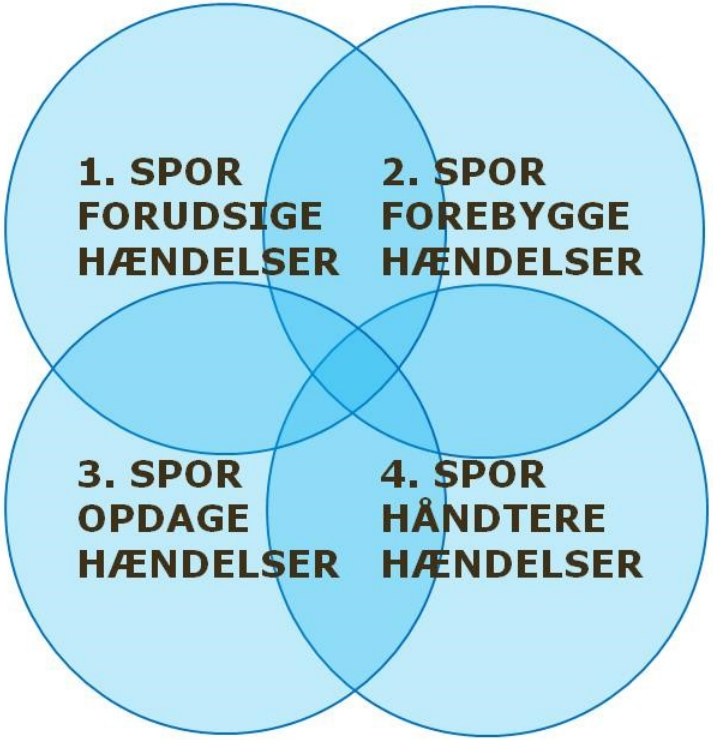
Gevinster ved det tværregionale samarbejde

- Der skabes et fælles tværregionalt fundament
- Eksempelvis politikker, skabeloner og modeller, som letter den enkelte regions arbejde med at styrke informationssikkerheden
- Øget juridisk compliance i regionerne - alle regioner arbejder løbende med at optimere arbejdsgange og rutiner i forhold til gældende lovgivning
- Regionerne står stærkere som forhandlingspart over for både eksterne og interne samarbejdspartnere
- Fælles og koordineret interessevaretagelse på området
- Regionerne lærer af hinanden og er med til at løfte hinanden inden for området.

Strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022

- Regionernes deltagelse i udarbejdelse af initiativer i cyberstrategien i 2018
- Udvalgte initiativer til indledende tværregionalt samarbejde:
  - 1.1 Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører
  - 1.2 Bedre overblik over sundhedssektorens sårbarheder og risici
  - 1.3 Effektiv koordination af varsler
  - 2.2 Styrket teknisk sikkerhed i sektorens løsninger og it-infrastruktur
  - 2.3 Håndtering af sikkerheden i ældre it-systemer og –udstyr
  - 3.1 Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr
  - 3.2 Etablering af overvågnings- og analysefunktioner
  - 3.3 Effektiv håndtering af mistanke om hændelser
- Arbejdsgrupper på tværs af sektorer

Strategiens 4 spor

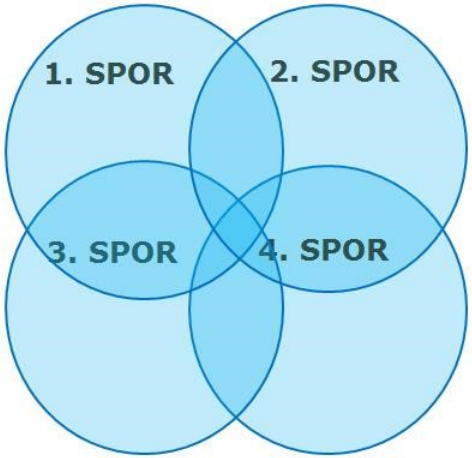


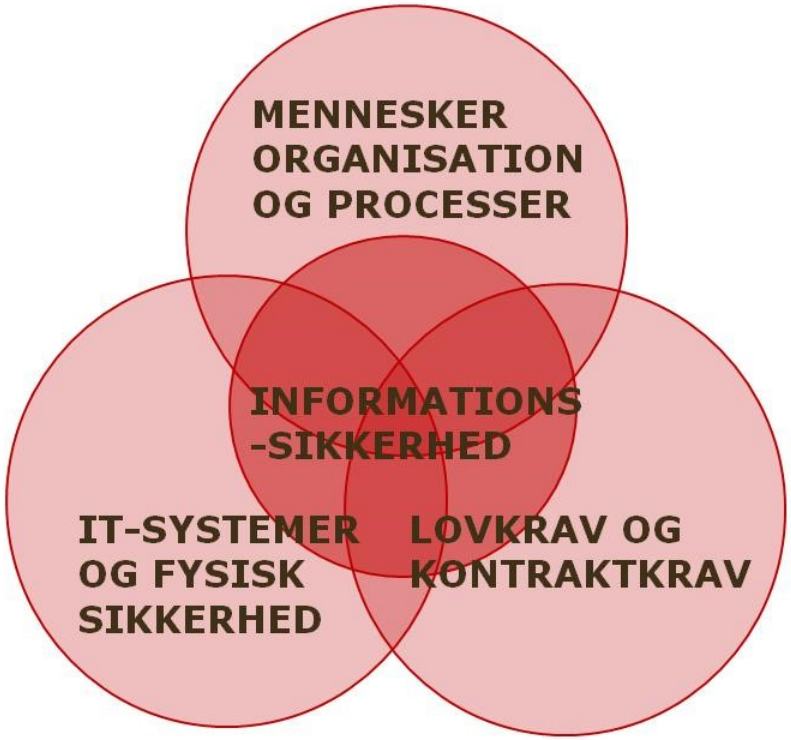
Strategien fortsat…

- PwC's analyse af strategiens omkostninger for regionerne
  - 2.2 Styrket teknisk sikkerhed i sektorens løsninger og it-infrastruktur
  - 2.3 Håndtering af sikkerheden i ældre it-systemer og –udstyr
  - 2.5 Skærpede sikkerhedskrav til it-leverandører
  - 2.6 Udbygning af sektorens sikkerhedsarkitektur
  - 3.1 Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr
  - 3.2 Etablering af overvågnings- og analysefunktioner
  - 4.1 Hændelseshåndtering
- Udfordringer vedrørende økonomi
- Udfordringer forbundet med prioritering af lokale initiativer vs. initiativer fra cyberstrategien

Det lange seje træk…

Cyberstrategiens spor vs. de tværregionale spor





Afrunding

- Sammenhold gør stærk
- Men vigtigt at man respekterer hinandens forskelligheder
- Prioritering af nationale tiltag ift. den lokale kontekst og problemstillinger
- Informationssikkerhed er et komplekst område og forudsætter typisk en forandringsproces (både teknisk og organisatorisk) bredt i regionen – det lange seje træk...
- En helhedsorienteret indsats