Risiko-og trusselsvurderinger i sundhedssektoren

Tanja Kaufmann
Sektionsleder DCIS Sund, Sundhedsdatastyrelsen

SUNDHEDSDATA-
STYRELSEN

Årets tema: Er tiden inde til at tale om en nødvendig digital omstilling af sundhedssektoren?

Risikovurderinger – But why?

Er det ikke bare de der folk fra sikkerhed, der er hysteriske?

Behandlingss

Forordningen kr
behandlings kar

Det er ikke dest
risikobaserede t
fysiske personer
forordningen

Vejledning om kriterier og krav til operatører af væsentlige tjenester i sundhedssektoren

Indledning

Bek

krav t

2. Sikkerhedsforanst

Operatører af væs
robusthed, tilgængel
væsentlige tjeneste.

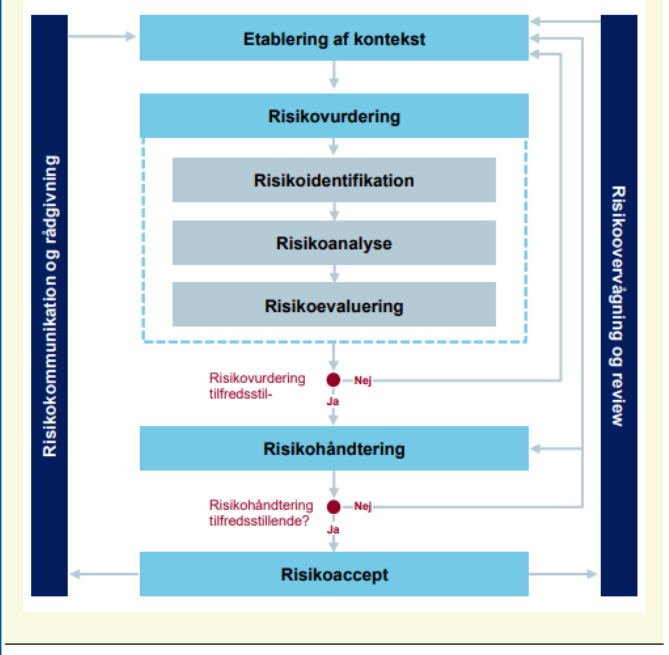
Dette sker på bagg
forstyrrende virkni
risikovurderingen s
væsentlige tjeneste.

ici for

NIS

ISO 27001

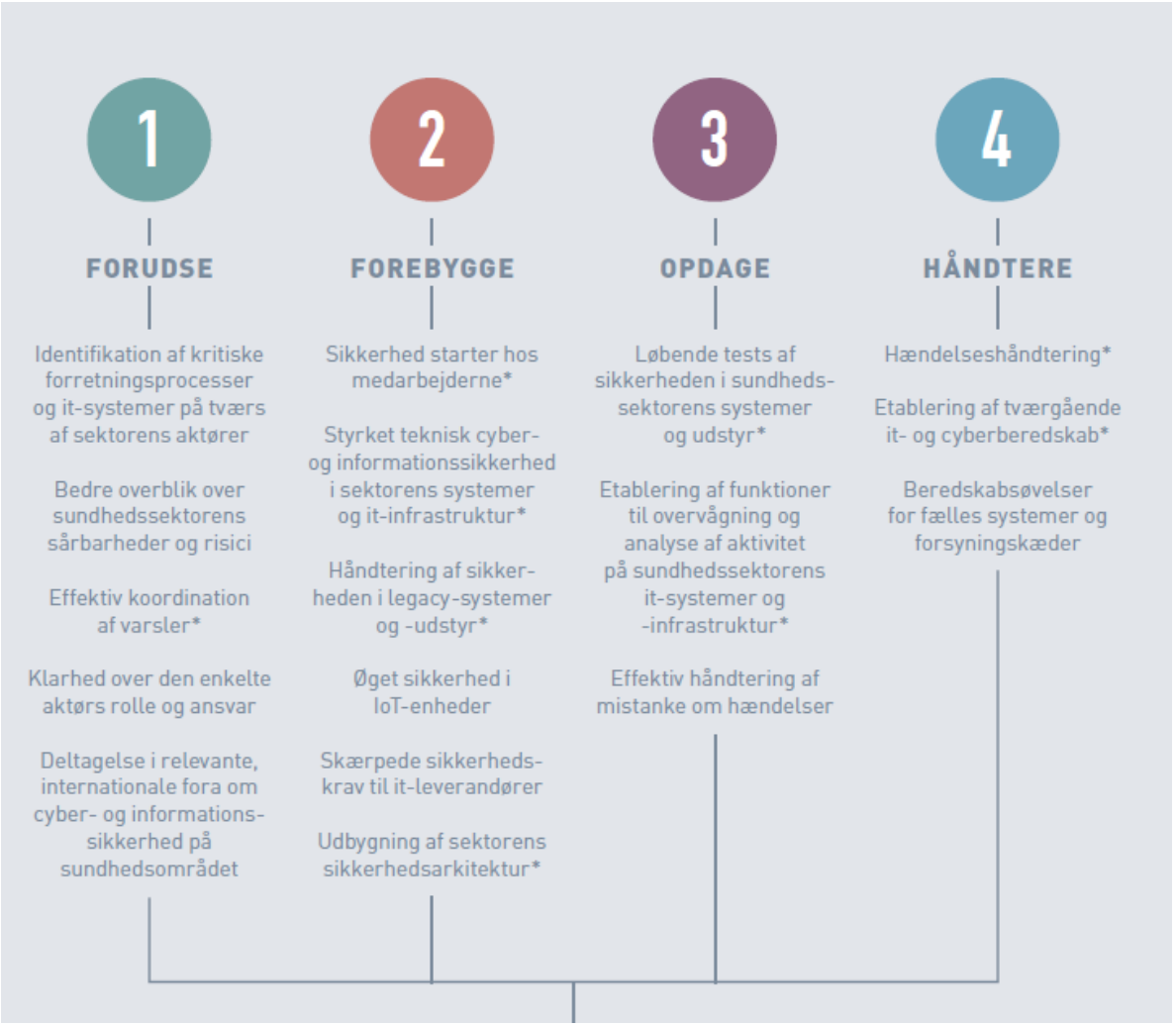
Figur 2.1
Illustration af risikostyringsprocessen



Kilde: Inspireret af ISO 27005

SUNDHEDSDATA-STYRELSEN

Et fælles fokus på tværs af sundhedssektoren



SUNDHEDSDATA-STYRELSEN

(For) Høje ambitioner (?)

INITIATIV 1.2.

Bedre overblik over sundhedssektorens sårbarheder og risici

Det er nødvendigt løbende at vedligeholde lokale og tværgående vurderinger af sårbarheder og risici. Det er de enkelte aktørers ansvar at udarbejde og opdatere egne sårbarheds – og risikovurderinger samt sikre ledelsesforankring. DCIS udarbejder i 2019 i samarbejde med sektorens aktører vejledninger til at understøtte arbejdet, således at vurderingerne over tid bliver metodisk ensartede. Vejledningerne vil desuden være obligatoriske at følge for sårbarheds – og risikovurderinger af fælles, prioriterede, kritiske systemer. DCIS har desuden til opgave at udarbejde den samlede sårbarheds- og risikovurdering for hele sektoren.

Vi tror stadig på opgaven

Indhold	For at skabe mest mulig værdi på tværs af sektoren og for de lokale aktører skal der i initiativet arbejdes med at forbedre metoden for indmeldelse af de lokale risikovurderinger til brug i udarbejdelsen af sektorens samlede risikovurdering. Fokus for metoden vil være samarbejde og vidensdeling mellem sektorens aktører for at berige et fælles overblik på tværs. De enkelte aktører udarbejder og opdaterer egne risikovurderinger. Sundhedssektorens trusselsbillede, der publiceres årligt af DCIS, kan anvendes i dette arbejde. Trusselsbilledet giver et grundlæggende overblik over aktuelle trusler og et indblik i trusselstendenser mod sundhedssektoren. Aktørernes sårbarheds- og risikovurderinger af den it-infrastruktur, der igennem initiativ 1.1 'Identifikation af sundhedssektorens samfundsvigtige funktioner og kritisk it-infrastruktur' identificeres som kritisk, skal som minimum være en del af aktørens samlede risikovurdering og dermed indgå i det samlede billede for sektoren.

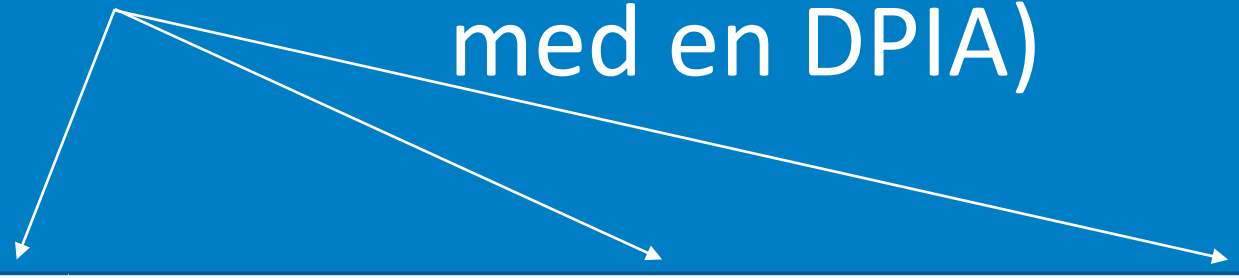
SUNDHEDSDATA-STYRELSEN

Det er et komplekst domæne!

SUNDHEDSDATA-
STYRELSEN

Metoden… Det ser enkelt ud, men lad dig ikke narre!

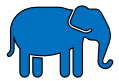
R = S (Sårbarheder og trusler) x K (konsekvensvurdering- ikke at forveksle med en DPIA)



Konsekvenser for forretningen?

Konsekvenser for den registrerede?

For samfundet (NIS)

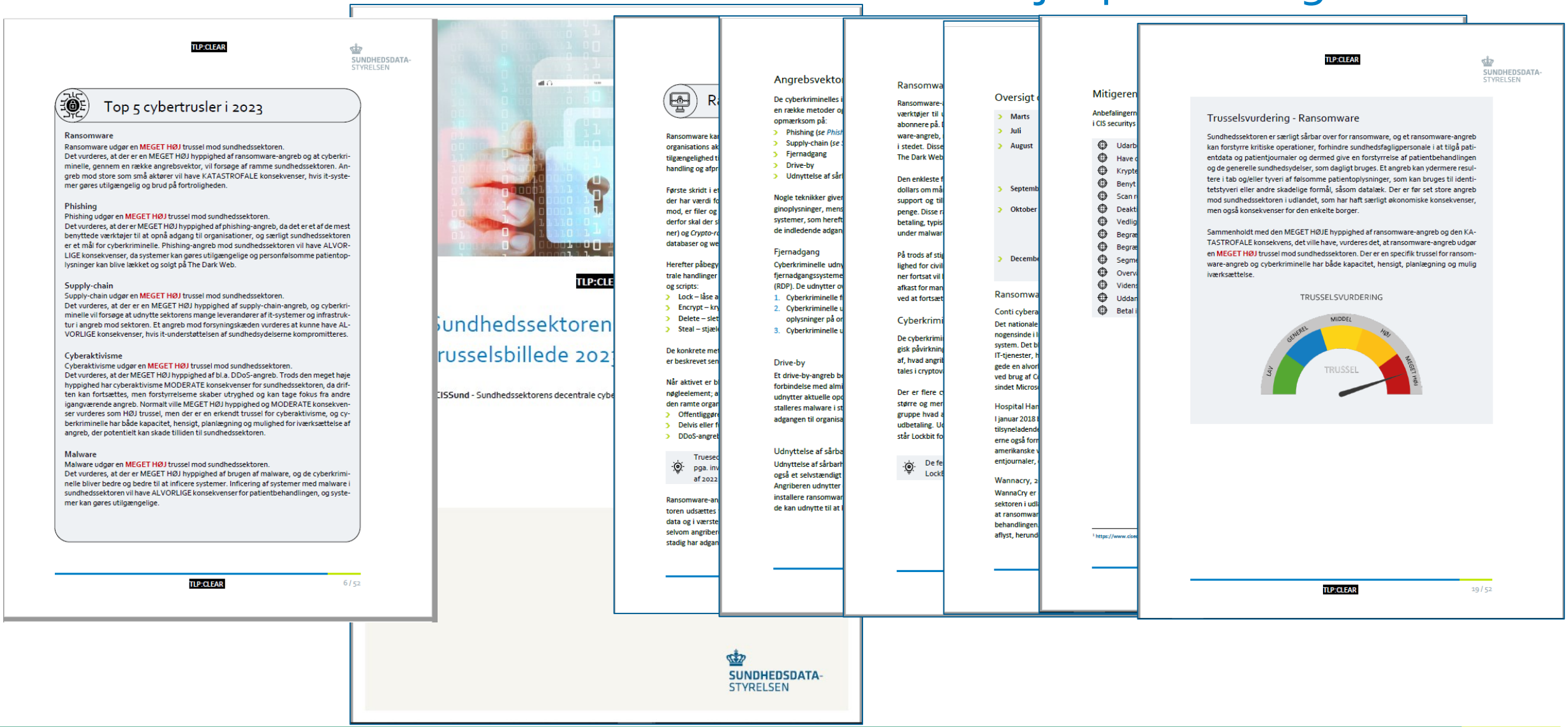
Spis elefanten i små bidder 

INITIATIV 1.2.

Bedre overblik over sundhedssektorens sårbarheder og risici

Det er nødvendigt løbende at vedligeholde lokale og tværgående vurderinger af sårbarheder og risici. Det er de enkelte aktørers ansvar at udarbejde og opdatere egne sårbarheds – og risikovurderinger samt sikre ledelses-forankring. DCIS udarbejder i 2019 i samarbejde med sektorens aktører vejledninger til at understøtte arbejdet, således a[redacted]e. Vejledningerne vil desuden være obligatoriske at følge for sårbarheds – og risikovurderinger af fælles, prioriterede, kritiske systemer. DCIS har desuden til opga-ve at udarbejde den samlede sårbarheds- og risikovurdering for hele sektoren.

Trusselsbilledet i sundhedssektoren – Hvordan hjælper det dig?



SUNDHEDSDATA-STYRELSEN

Vi starter med en sammenlignelig mapning

– taxonomy of operational cyber security risk v.2

1. Action of people	2. Systems and Tecnhology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disaster**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
	2.1.4 Obsolescene	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2 Deliberate		3.1.5 Information flow	4.1.5 Unrest
1.2.1 Fraud	**2.2 Software**	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.2 Sabotage	2.2.1 Compatibility	3.1.7 Service level agreements	
1.2.3 Theft	2.2.2 Configuration management	3.1.8 Task hand-off	**4.2 Legal issues**
1.2.5 Vandalism	2.2.3 Change control		4.2.1 Regulatory compliance
	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3 Inaction	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.1 Skills	2.2.6 Testing	3.2.2 Metrics	
1.3.2 Knownledge		3.2.3 Periodic review	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.4 Process ownership	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design		4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	
	2.3.4 Complexity	3.3.2 Funding	**4.4 Service dependencies**
		3.3.3 Training and development	4.4.1 Utilities
		3.3.4 Procurement	4.4.2 Emergency services
			4.4.3 Fuel
			4.4.4 Transportation

Niveau 1.	1. Action of people
Niveau 2.	1.1 Inadvertent
Niveau 3.	1.1.1 Mistakes

	A	B	C	D	E	F	G	H	I	J	K	L
1	År og aktør		System		Trusselskatalog og risikobeskrivelse				Risikoindeks			Uddybning
2	År*	Aktør*	Tjeneste*	Net- og informationssystem*	Niveau 1 (x)*	Niveau 2 (x.x)*	Niveau 3 (x.x.x)	Beskrivelse af risiko*	Sandynlighed*	Konsekvens*	Risikoscore*	Kommentar
3	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*					lav	høj	8	*Kommentar til risikoen*
4	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*					Meget høj	Mellem	15	*Kommentar til risikoen*
5	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*					Lav	Lav	4	*Kommentar til risikoen*
6	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
7	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
8	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
9	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
10	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
11	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
12	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
13	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
14	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
15	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
16	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
17	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
18	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
19	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
20	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
21	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
22	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
23	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
24	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
25	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
26	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
27	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
28	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
29	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
30	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
31	2023	*Indsæt aktør*	*Indsæt tjeneste*	*Indsæt systemnavn*								*Kommentar til risikoen*
32												

Overblikket

SUNDHEDSDATA-STYRELSEN

Med hvad så med den ensartede metode?

- Der er lavet en afgræsning i målgruppen, som betyder at,
  - Der arbejdes videre på 4. år i en arbejdsgruppe på tværs af aktører underlagt NIS (1) i sundhedssektoren
  - Vi er blevet enige om metodefrihed
  - Fokus er på at skabe fælles referencetabeller, der giver sammenligningen resultater.

- Gevinsterne er bl.a.,
  - Understøttelse af det lokale arbejde
  - Indsatser og prioriteringer kan ske på et oplyst grundlag
  - Et samlet kvalificeret risikobillede.

Kontakt

E-mail

DCISSUND@sundhedsdata.dk

Mere information

Cyber- og informationssikkerhed i sundhedsvæsenet

SUNDHEDSDATA-
STYRELSEN