Sikkerhedskultur

Webinaret starter kl. 14.00

Webinaret

Tema: Sikkerhedskultur

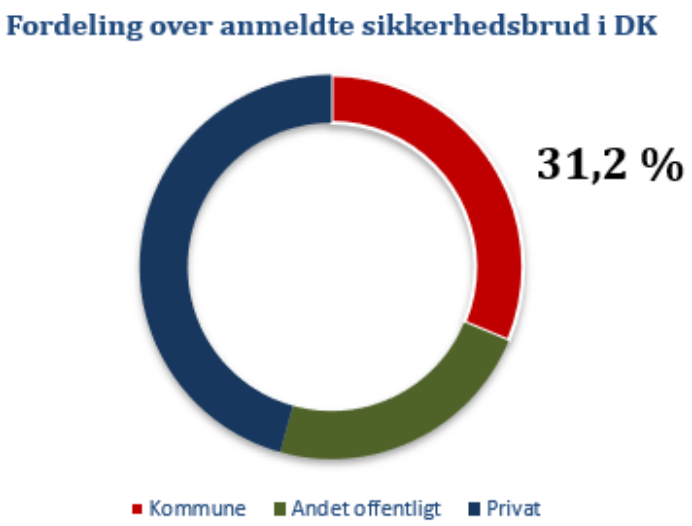
Nogle svar på:

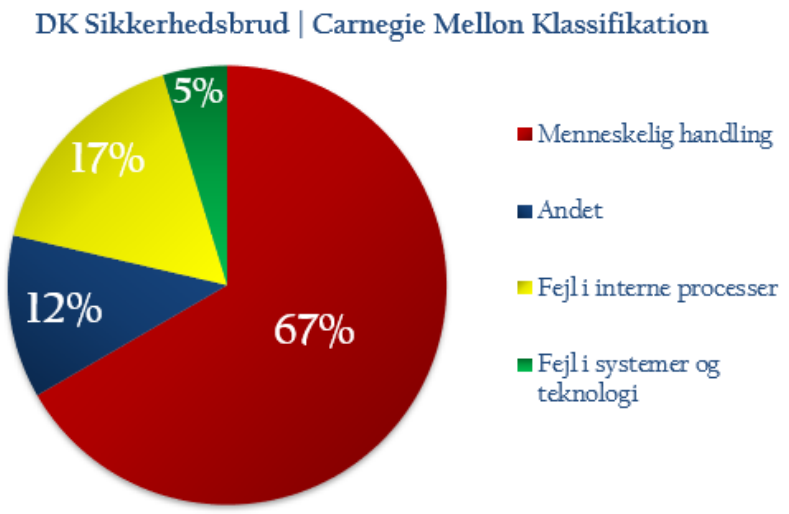
- Risikostyring af det ”fjerde element” - ansatte
- Sikkerhedsorganisationen
- Kultur
- Effekt af fokus på kultur

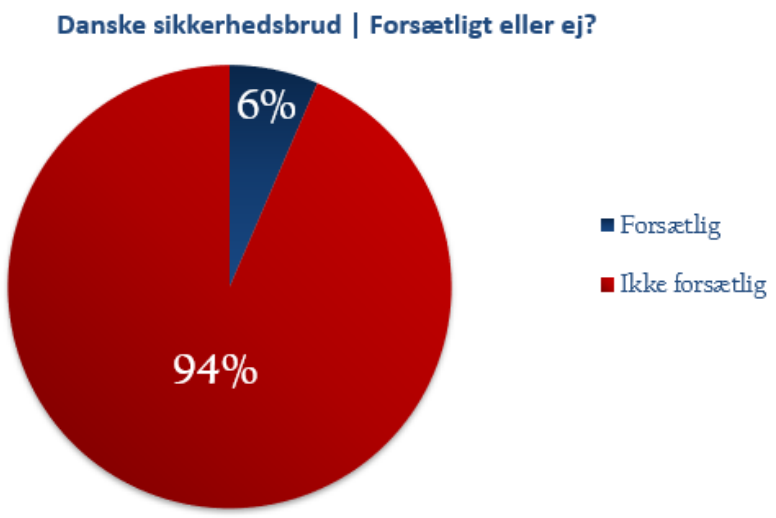
Klaus Kristensen
Direktør I-Trust
Ekstern Lektor Aalborg Universitet

Årsag til brud

DATATILSYNET





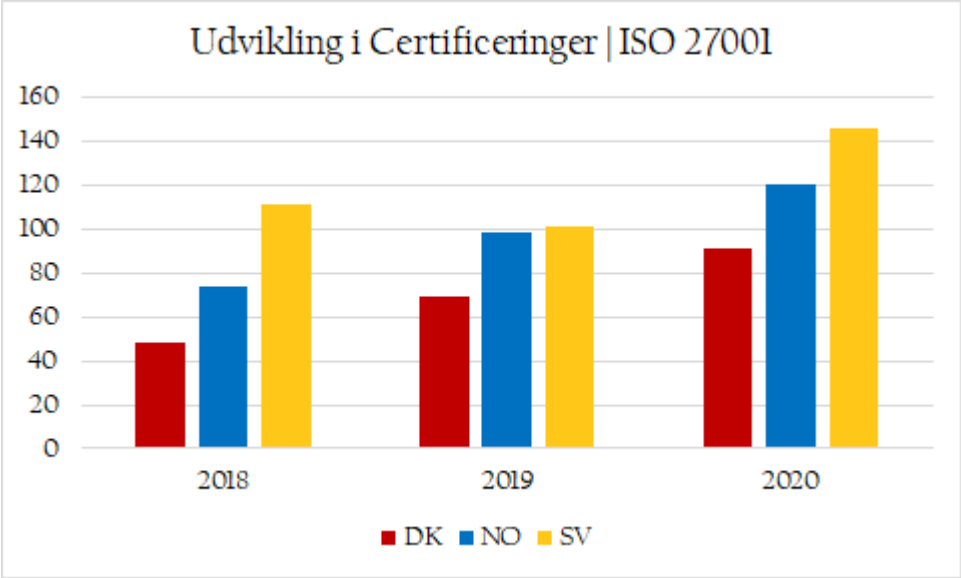


Paradoks

Store dele af det eurpæiske og danske sikkerhedsarbejde tager afsæt i ISO 27001 - men der er meget få certificeringer – også set ift. første udkast kom i 2005 (på en ramme fra 1995)

ISO SURVEY 2020

	ISO 9001		ISO 27001	
	Standard for kvalitetsstyring		Ledelsesstandard for informationssikkerhed	
	Certificeringer	*Lokationer*	*Certificeringer*	*Lokationer*
DK	2181	7363	81	198
NO	2578	4952	120	252
SV	3190	10761	146	400

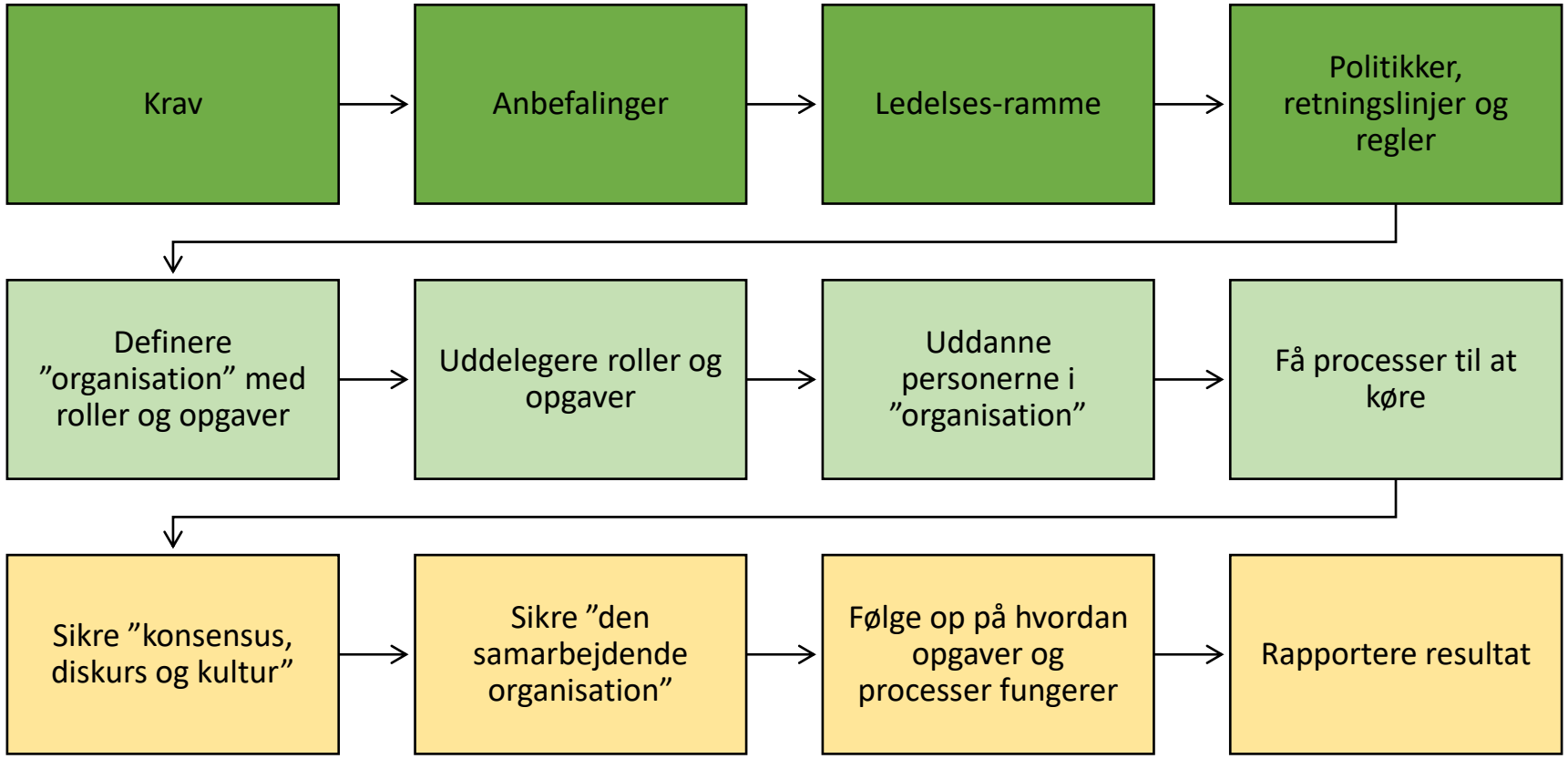


Undersøgelser peger på, at årsagen skal findes i manglende kompetencer, ansvarsfordelinger og ressourcer.

Jo længere væk fra 2018 …

Aktuel undersøgelse af dagstilbudsområdet i en dansk kommune

Fra baselineundersøgelserne



Adfærd

Det vi gerne vil undgå …

Korte effektive læringsprogrammer …

Venlige påmindelser …

Sanktioner …

Gør vi det rigtigt?

Det korte svar er, at vi kan gøre mere:

- Vi risikostyrer, hvor der er mindst risiko: systemer og fysiske ressourcer
- Vi overser den største risiko: menneske og organisationer
- Standarderne hjælper os ikke – præmissen er, at organisationer gør det forventede
- Vi ”hælder” ukritisk awareness kurser afsted – uden at kendeudfordringen

Hvis vi gør mere og får mere fokus på den menneskelige faktor:

- Færre og mindre tab
- Færre ”beredskabsomkostninger” til genopretninger
- Bedre behandlingsprocesser og trygge borgere

Dagens tema

Hvordan kan vi kvantificere og dermed kvalificere indsatser for:

- Governance - indeks
- Leder - indeks
- Adfærd - indeks
- Kompetence - indeks
- Hændelse/rapportering - indeks
- Behandlings-sikkerhed - indeks

I-Trust løsninger

I-TRUST

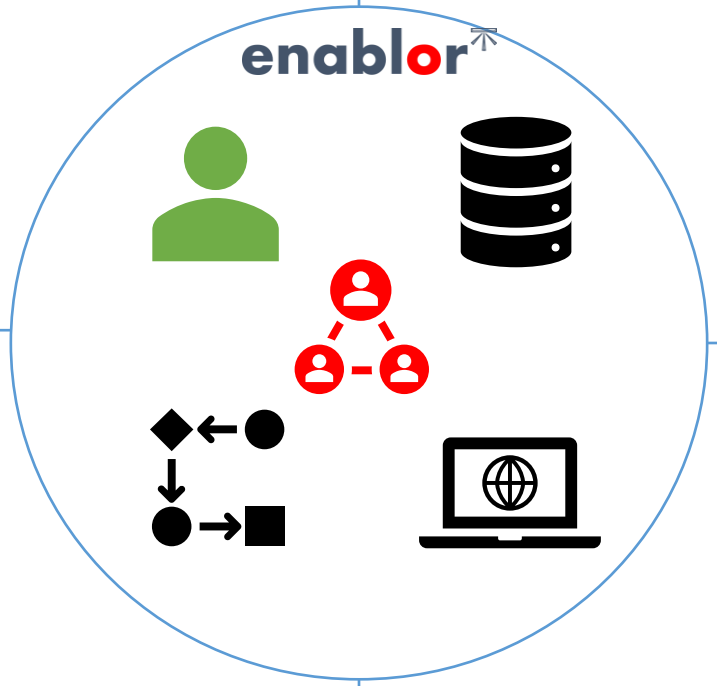
SIO: Roller og ansvar
KFE: Sikkerhedskultur

Awareness programmer
GDPR læring

Kompetenceprogrammer for systemejerne

Organisation

Indsats



KL

KL Baseline

Baseline +

ISO 27001
GDPR
Cybersikkerhed
SiO
+ IoT
+ AI & Bigdata
+ Sundheds-IT

enablor GRC

Interne audits
Leverandørstyring
Sikkerhedsstyring
GDPR-styring og dokumentation
Risikostyring

Risiko / compliance

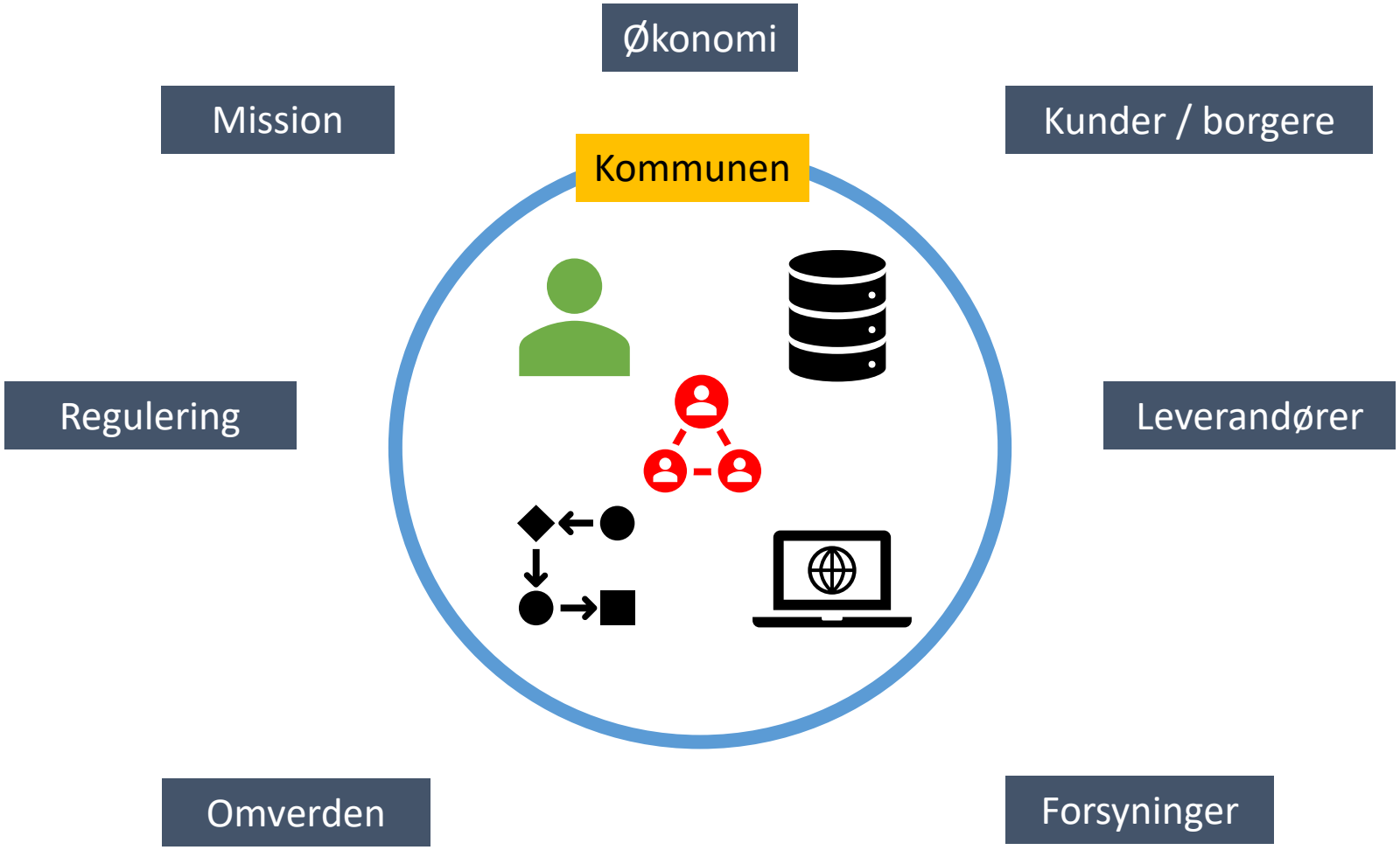
Auditering

digital tryghed

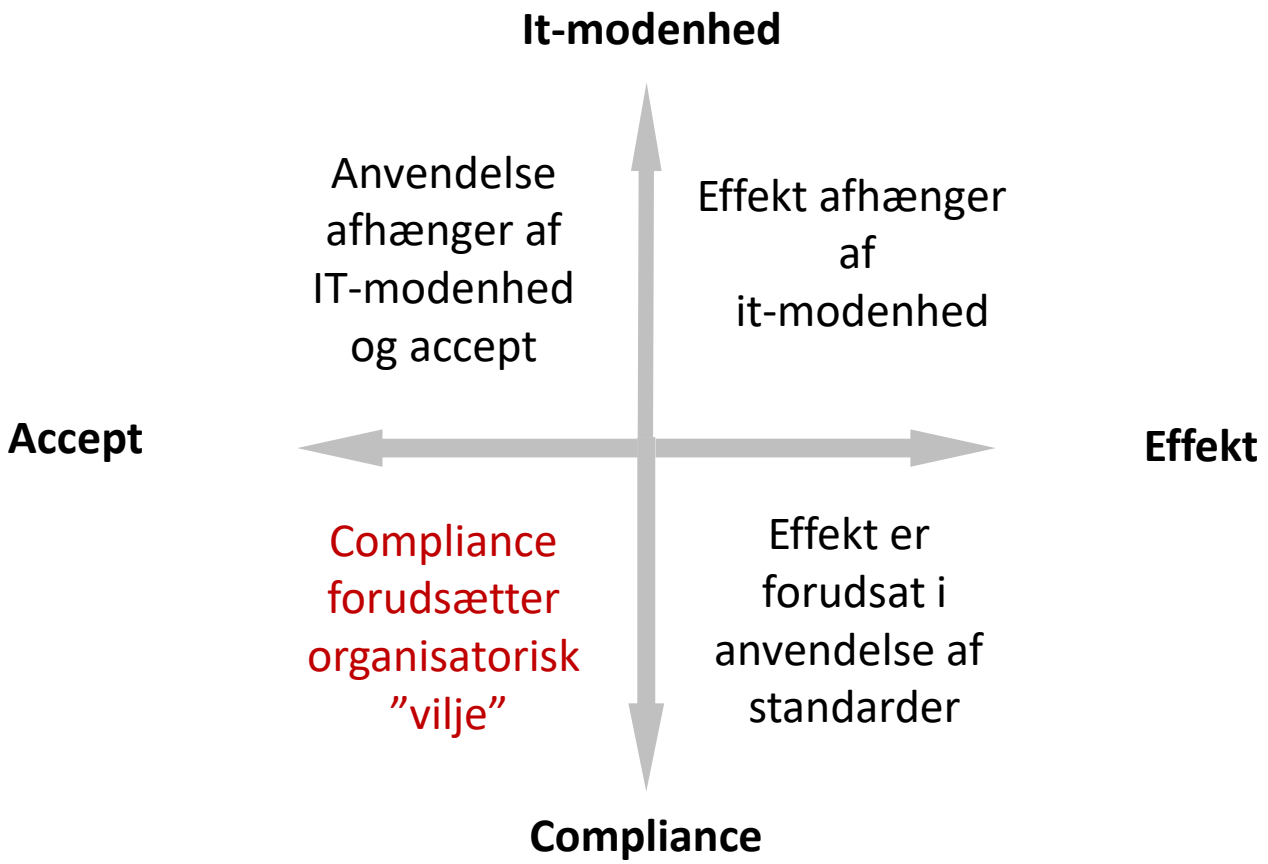
DATATILSYNET

Kultur og organisation

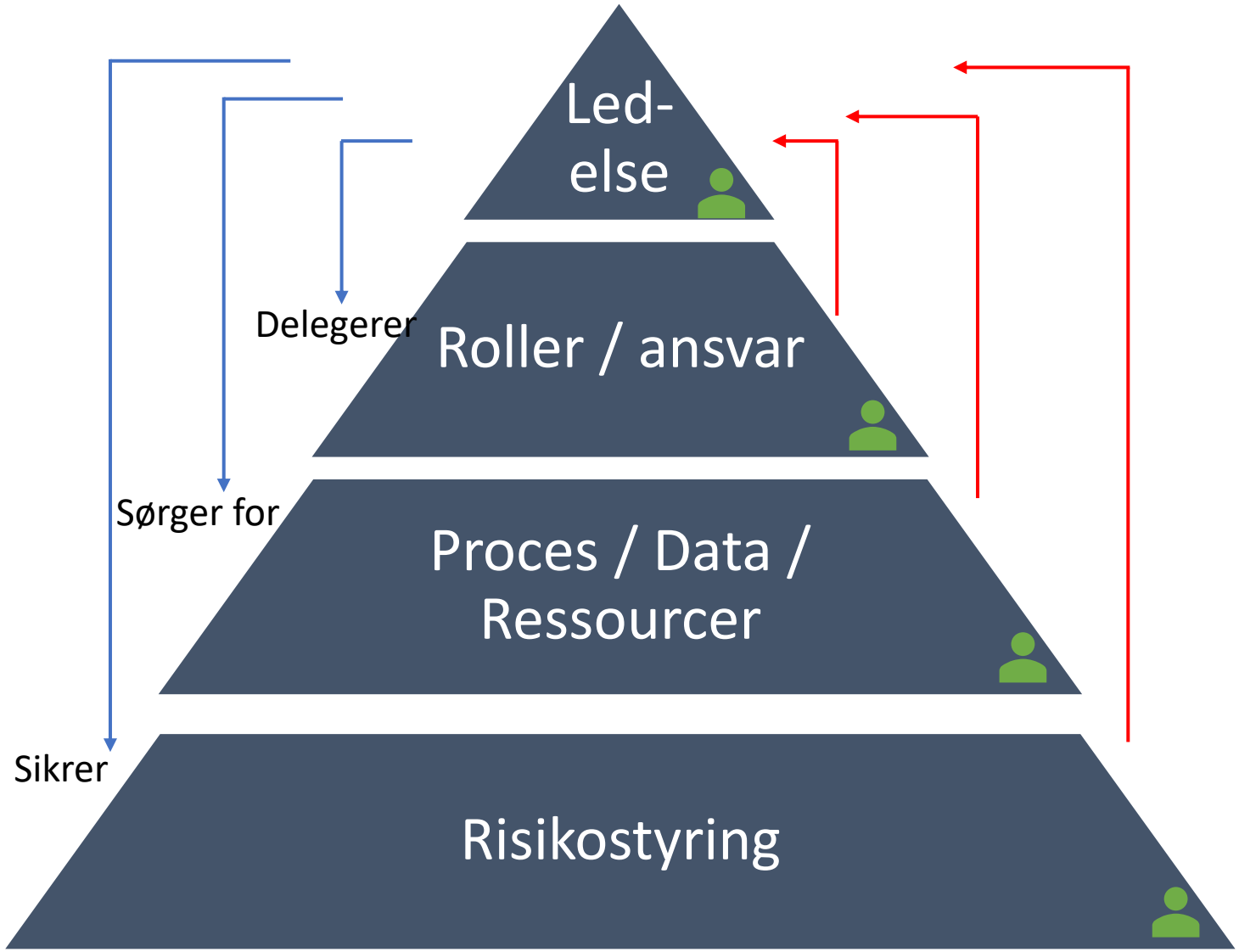
Virksomheden



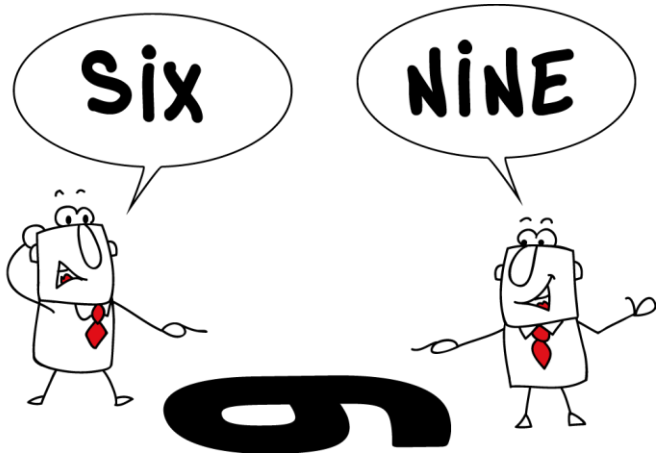
Parametre i informationssikkerhed



Ledelsens opgaver
Governance



Konsensus, diskurs, kultur



Den ansatte:
Diskurs og kultur

Ideal verden

Etisk diskurs

Politisk diskurs

Individ

Kollektiv

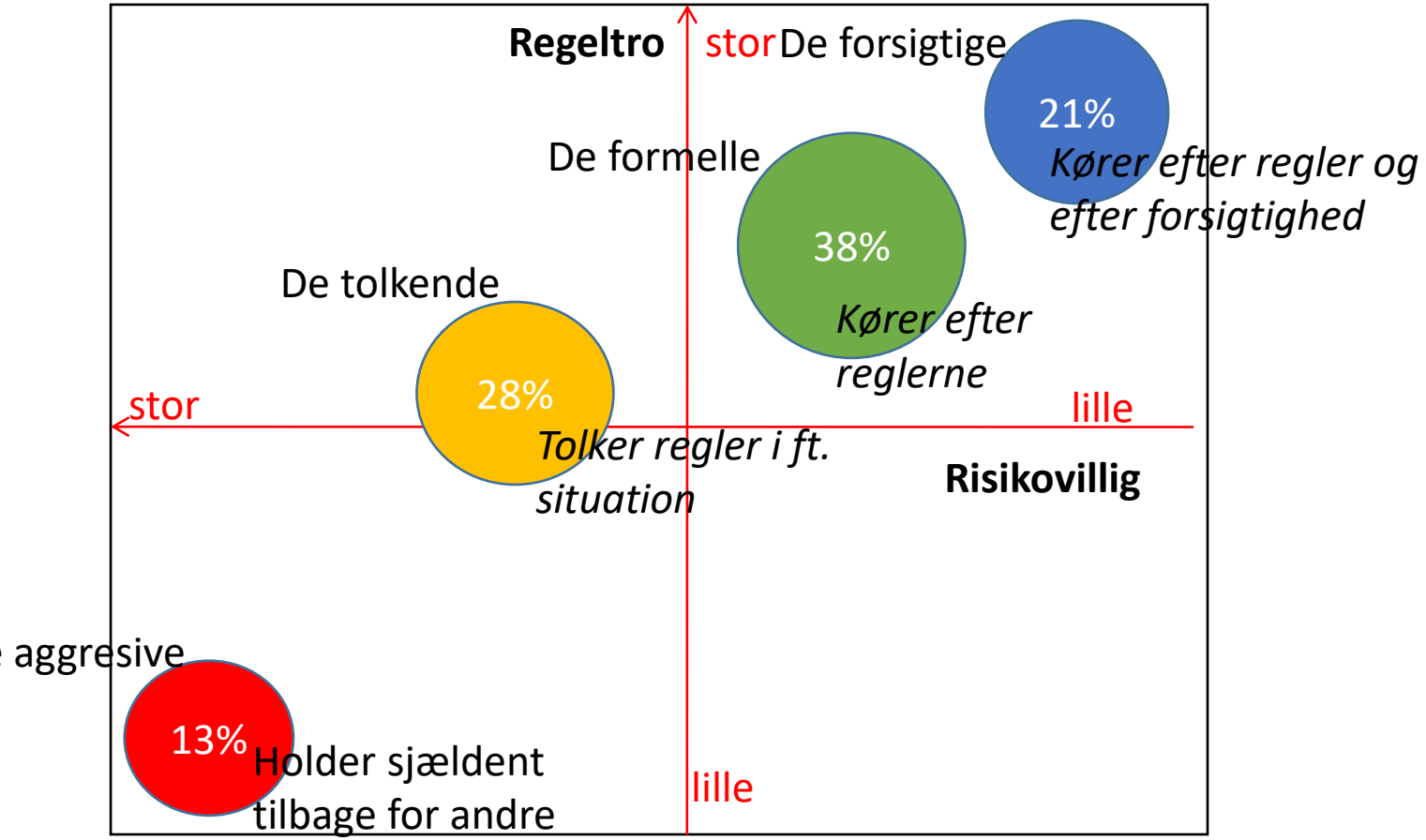
Pragmatisk diskurs

Økonomisk diskurs

Pragmatisk verden

Adfærdstyper

Trafikstudier



MORGENAVISEN Jyllands-Posten

Den forsigtige

Iben Madsen, 37 år, Viby:
Jeg overholder selvfølgelig fartgrænserne, for jeg gider ikke bruge penge på fartbøder. Men jeg tror, mange kører for stærkt, fordi de glemmer at holde øje med farten, eller måske synes de, at de bare følger trafikken.

Den tolkende

Peter Klein, 42 år, Hørning:
Jeg kører ikke for stærkt i byen, for trafikken er ofte tæt, og man skal jo holde ved lyskrydsene hele tiden alligevel. Bøden stiger også hurtigt, hvis man kører stærkt i byen. Men andre steder glider det bare bedre, hvis man kører 80 km/t i stedet for 70, som måske er

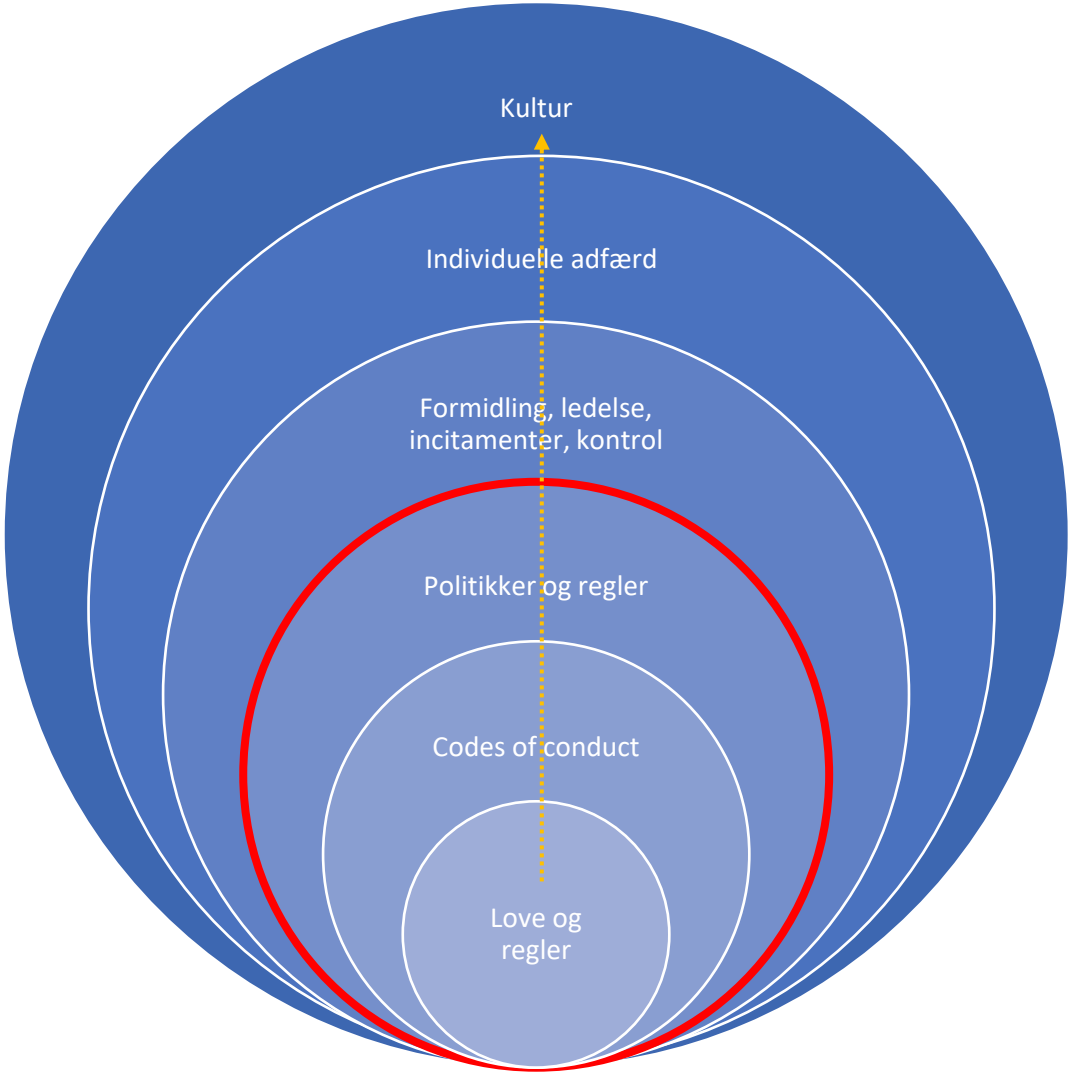
Den lovlydige

Lars Kolling, 53 år, Malling:
Selvfølgelig kører jeg for stærkt indimellem. Nogle steder passer det bedre til forholdene at køre 60 eller 70 km/t, mens det andre steder er vildt bare at køre de tilladte 50 km/t. Jeg retter mig efter forholdene, ikke skiltene.

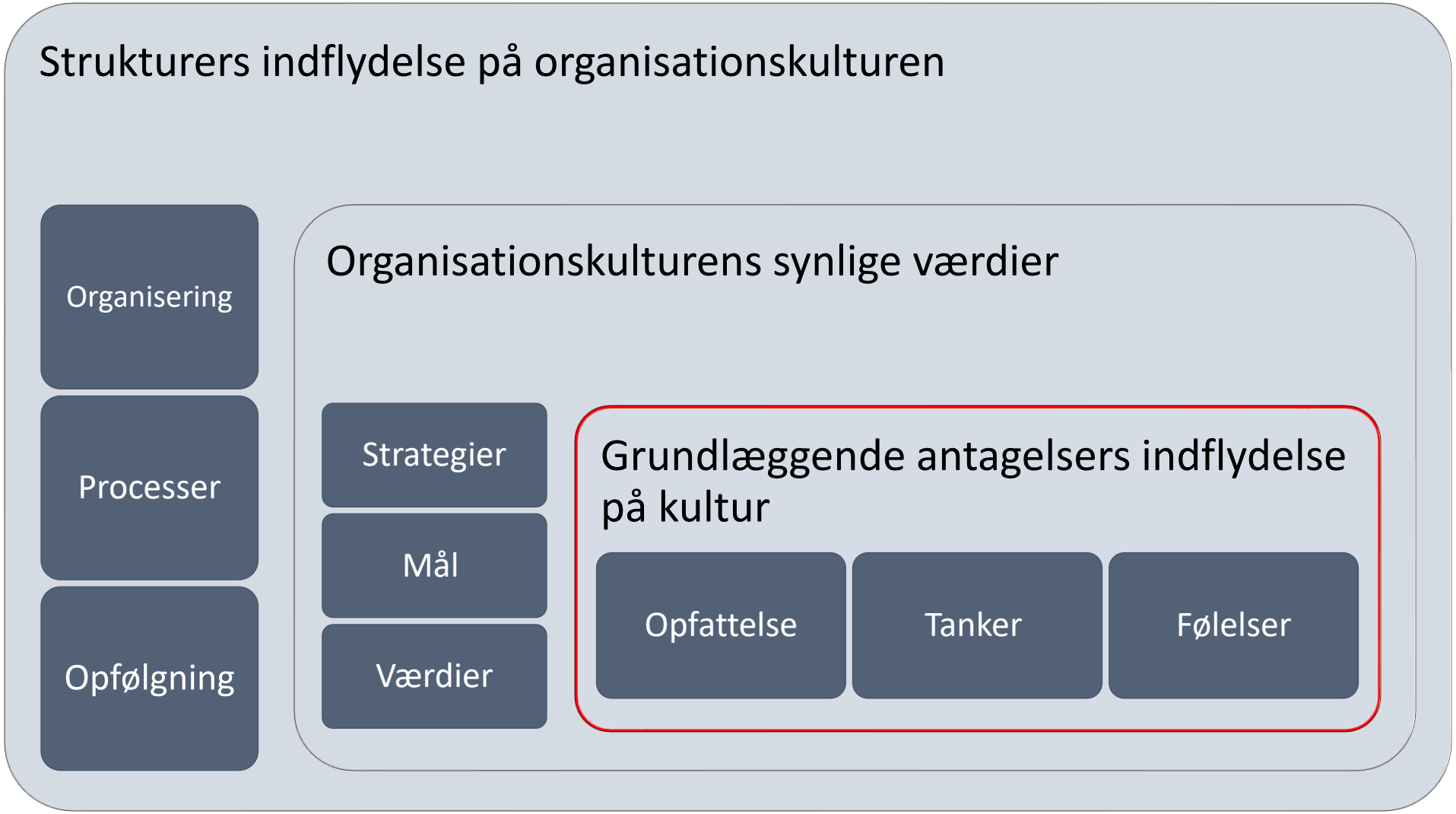
Den aggressive

Per Andersen, 45 år, Herning:
Jeg kører meget sjældent for stærkt i byerne. Men på landevejen sker det da, at det går lidt for stærkt. Jeg kommer fra "det vilde vesten", og der er det nok meget almindeligt at køre for stærkt. Vi er ikke som svenskerne og nordmændene – vi er ikke opdraget til at holde den slags regler.

Risikokultur



Kultur-”komponenter”



KFE platformen

KFE projekter

Udviklet i samarbejde med:

OKON – psykologer
fra Århus Universitet

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

enisa European Network and Information Security Agency

NorSIS Norsk senter for informasjonssikring

HELSE SØR-ØST

norskhelsenett

DIGITALISERINGSSTYRELSEN

Ministeriet for Fødevarer, Landbrug og Fiskeri
Fødevarestyrelsen

VIBORG KOMMUNE

KFE - komponenter

Personlige attributter:
Køn, Alder, Anciennitet, Magtaccept, Risikovillighed, …

Kendskab til regler → Accept af regler → Evne til at udføre opgave ift. teknologi og regler → Vilje til at ville efterleve regler → Udførelse i situationen

Ydre attributter:
Sanktioner, Kontrol, Ledelsens tydelighed, Formidling

KFE metoden

Fælles KFE ramme til ledere og ansatte
Særlige opfølgningsområder til lederne

Personlige
- Køn
- Alder
- Anciennitet
- Risikovillighed

Generelle
- Organisation
- Arbejdsområde
- Følsomme / fortrolige data
- Lederen

Kendskab
- Tema 1 – f.eks. Sociale medier
- Tema 2 – f.eks. Mail
- Tema 3 – f.eks. kodeord

Forståelse
- Tema 1 – f.eks. Sociale medier
- Tema 2 – f.eks. Mail
- Tema 3 – f.eks. kodeord

Efterlevelse
- Tema 1 – f.eks. Sociale medier
- Tema 2 – f.eks. Mail
- Tema 3 – f.eks. kodeord

Risikovillighed

Ledelsen

Kompetencer

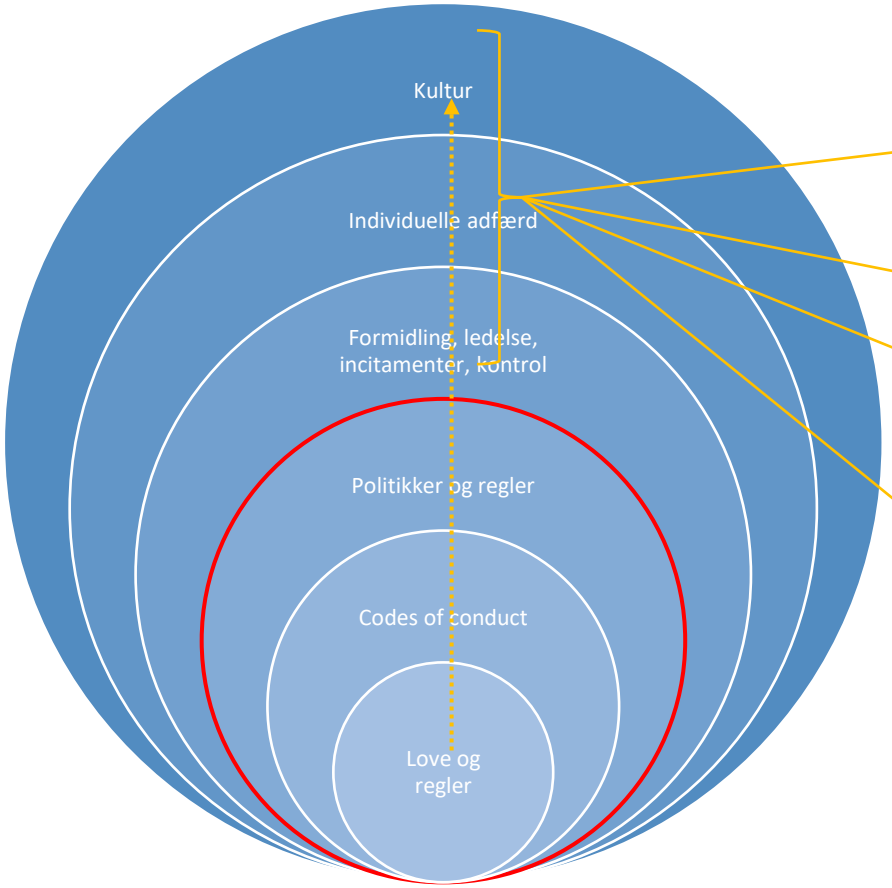
Adfærd

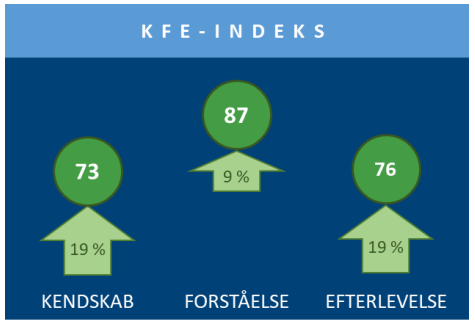
KFE-undersøgelser

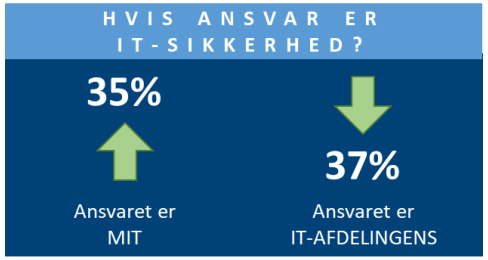
Indeks-niveau	Karakteristik	
70 - 100	Forstår og efterlever i høj grad politikker og regler	Høj
40 – 69	Har en vis opmærksomhed på politikker, men mangler dybere kendskab og forståelse for nødvendigheden af regler	Middel
0 – 39	Politikker har ingen væsentlig betydning, og man har ikke tilstrækkelig indsigt i regler	Lav

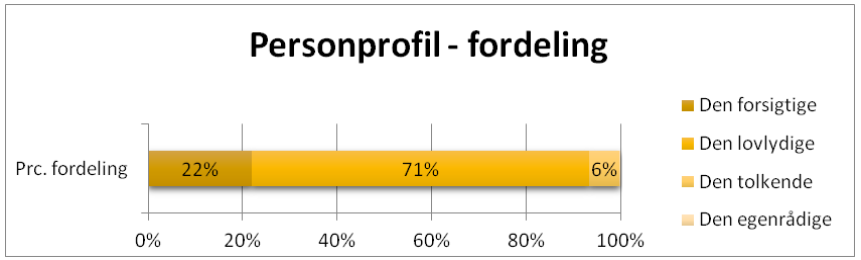
Spørgsmålene fortolkes på en skala fra 1 til 5, der indekseres på en 100 point skala.

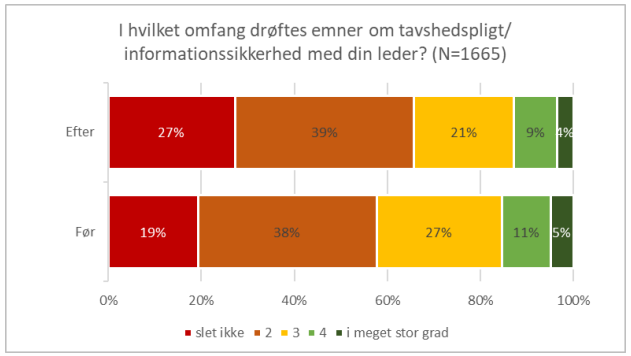
Eksempler på KPI

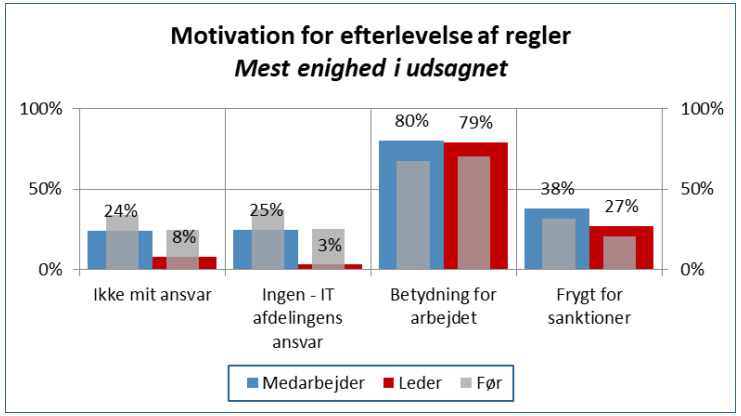




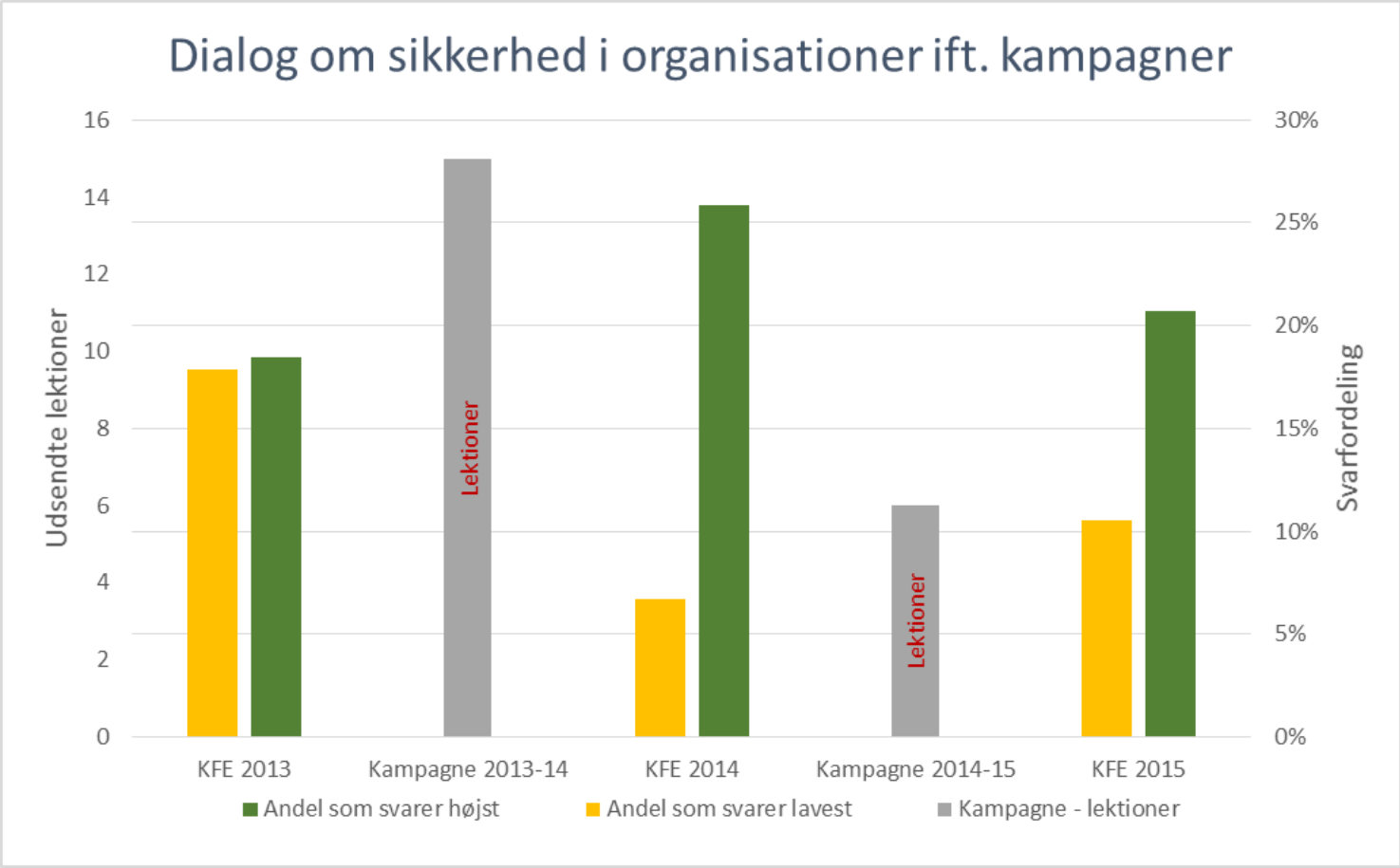




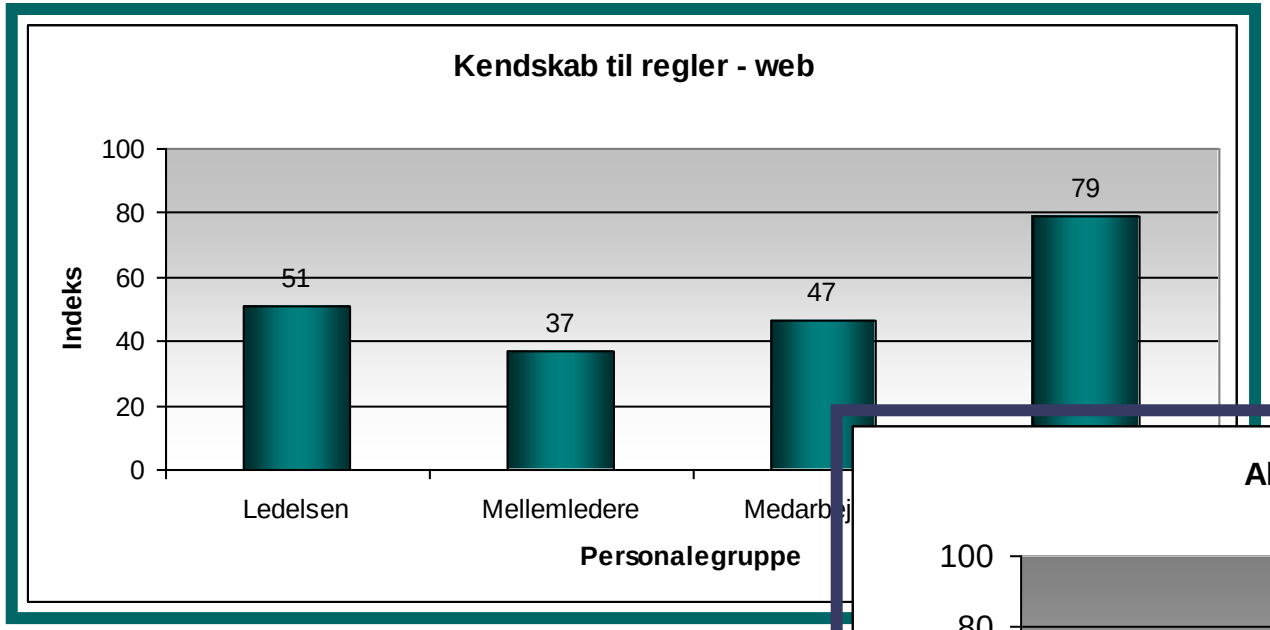


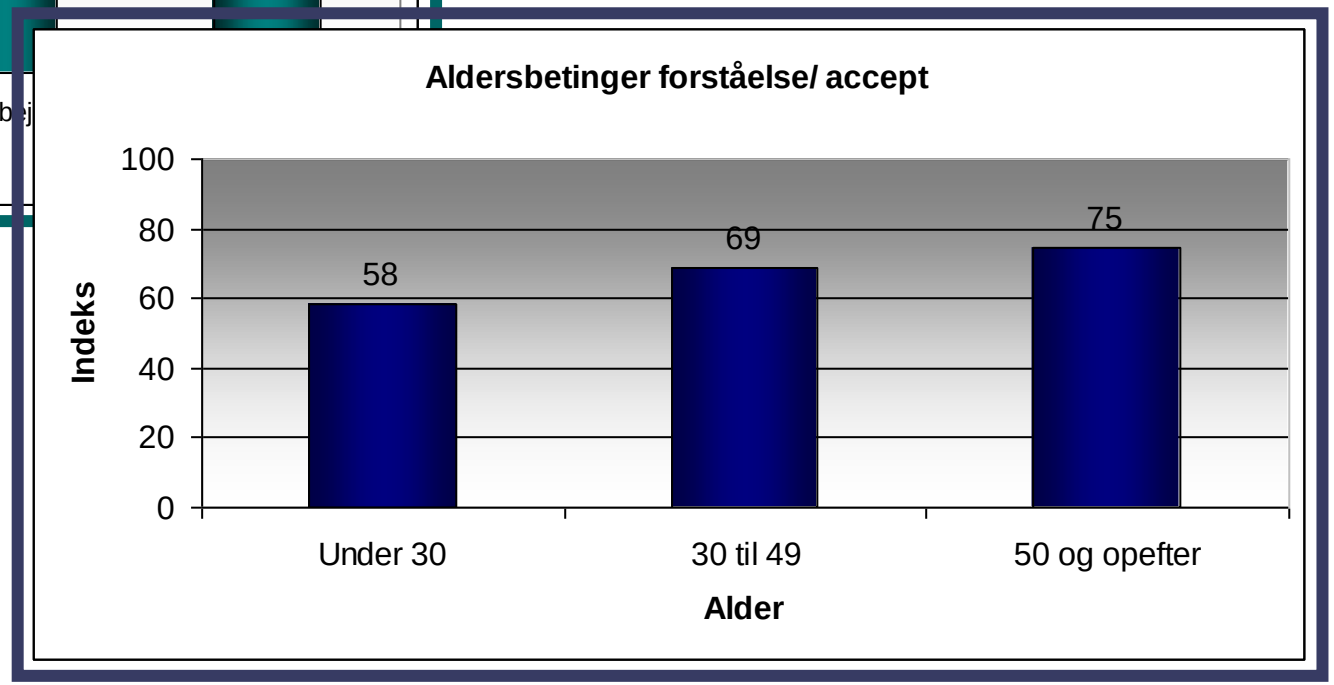


KFE- Effekt


Dialog om sikkerhed i organisationer ift. kampagner
Udsendte lektioner
Svarfordeling
16
14
12
10
8
6
4
2
0
30%
25%
20%
15%
10%
5%
0%
Lektioner
Lektioner
KFE 2013
Kampagne 2013-14
KFE 2014
Kampagne 2014-15
KFE 2015
Andel som svarer højst
Andel som svarer lavest
Kampagne - lektioner

Flere eksempler





Forløb ved et KFE projekt

Opret organisation ved indlæsning fra AD, …

Tilpas spørgeskema:
Tema
Egne tekster
Link til politikker

Udsend og besvar
KFE undersøgelse

Onepager til hver deltager

Onepager til leder over egen afdeling

Sårbarhedsvurderingsrapport til projektejeren

Filter
Filter brugere

Personer i Kommune (demo)

+ Indlæs personer

Primær organisation	Navn	E-mail	KFE	SIO	Status	Handlinger
Kommune (demo)	Kristian Beri				Aktiv	
Kommune (demo)	Kasper Niels				Aktiv	
Kommune (demo)	Niels Mikkel				Aktiv	
Kommune (demo)	Amin Barrac				Aktiv	
Kommune (demo)	Anders Møll				Aktiv	
Kommune (demo)	Jakob Brink				Aktiv	
Kommune (demo)	Marc Stagst				Aktiv	

Brugere per side: 10 1 - 10 Af 14

+ Indlæs personer

Indlæs fra

- ○ Active Directory (AD)
- ◉ CSV-fil

Upload

Træk fil hertil eller tryk for at uploade

Anuller Indlæs

Opret organisationsaktivitet

1 Oplysninger — 2 Tildeling — 3 Påmindelser — 4 Resume

Tildel aktiviteten

Vælg hvad aktiviteten vedrører, og tildel den til bestemte personer i din organisation. Hver tilføjet person vil modtage deres egen aktivitet de kan gennemføre. Den ansvarlige kan se status på hver persons gennemførelse af aktiviteten i tabeloversigten

Aktiviteten vedrører

Organisationsbesvarelse
KFE Undersøgelse til systemejere

Aktiviteten er tildelt

Oplysninger om personer, deres rolle og system

Navn	Rolle	Email	Systemer
Person1	Systemejer	Email@email.dk	Kommunesystem
Person2	Systemejer	Email@email.dk	Kommunesystem2
Person3	Systemejer	Email@email.dk	Kommunesystem3

Personer per side: 5 1 - 1 Af 1

Forrige Næste

Organisationsaktivitet over KFE Undersøgelse til systemejere

Aktiv

Oplysninger

Organisationsaktivitet over KFE Undersøgelse til systemejere

Kim Pedersen

10/11/21 - 30/11/21

KFE Undersøgelse til systemejere

Beskrivelse

Der skal laves rutinemæssigt kontrol af kendskab, forståelse og efterlevelse af vores informationssikkerhed i organisationen

Aktiviteten er tildelt til

	Navn	Enhed	Påmindelse	Status	Gennemførelse	Handlinger
	Person1	Kommune (demo)	✓	Aktiv 4d	67%	⋮
	Person2	Kommune (demo)	✓	Aktiv 4d	71%	⋮
	Person3	Kommune (demo)	✓	Færdig	100%	⋮

Anuller | Gem & luk

Du svarer for:

Marc Stagsted Mogensen

100%

1 KFE Undersøgelse
- Generelt
- Email
- Sociale medier
- Adgangskoder

2 Resume

Informationssikkerhedspolitik

I hvilket omfang taler du med din leder om tavshedspligt/ informationssikkerhed?

I nogen grad

Ved ikke
Kan ikke besvares

Kommentar

Sørger du for at holde dig ajour med organisationens informationssikkerhedspolitik?

I nogen grad

Ved ikke
Kan ikke besvares

Hindrer retningslinjerne for informationssikkerhed dig i dit daglige arbejde?

I nogen grad

Ved ikke
Kan ikke besvares

Referencer, hjælp og vejledning

Hjælpetekst
Det kræver et kendskab til organisationens informationssikkerhed, for at kunne vurdere omfanget

Du svarer for:

Marc Stagsted Mogensen

100%

1 KFE Undersøgelse

2 Resume

Resume

Du har udfyldt besvarelsen **100%** og fået et samlet resultat på **79/100**. Nedenfor finder du et resume af din besvarelse.

Hent rapport

Resultat

Generelt	RESULTAT: 43
Email	RESULTAT: 30
Sociale medier	RESULTAT: 27
Adgangskoder	RESULTAT: 11

Forrige

Afslut tilsyn

Filter
Filter brugere

Personer i Kommune (demo)

+ Indlæs personer

Primær organisation	Navn	E-mail	KFE	SIO	Status	Handlinger
Kommune (demo)	Kristian Bering Asmussen	demo_bl@i-trust.dk	93	48	Aktiv	⋮
Kommune (demo)	Kasper Nielsen	knielsen@i-trust.dk			Aktiv	⋮
Kommune (demo)	Niels Mikkelsen	mikkelsen_demo@i-trust.dk	52		Aktiv	⋮
Kommune (demo)	Amin Barrada	barrada@i-trust.dk	78		Aktiv	⋮
Kommune (demo)	Anders Møller Thomsen	thomsen_bl@i-trust.dk	23		Aktiv	⋮
Kommune (demo)	Jakob Brink	brink_bl@i-trust.dk			Aktiv	⋮
Kommune (demo)	Marc Stagsted Mogensen	mogensen_bl@i-trust.dk			Aktiv	⋮

Brugere per side: 10 1 - 10 Af 14

Udtræk rapport for statusvurdering

Vælg rapport type
Spørgerammer

Undersøgelse

Vælg undersøgelse
KFE 2021

Vælg spørgeramme
KFE Undersøgelse

Medtag ikke-frigivne svar? ☐

Organisation

Vælg besvarelsesår
2021

Vælg organisation
Kommune (demo)

Selektion

Vælg KLE-nummer

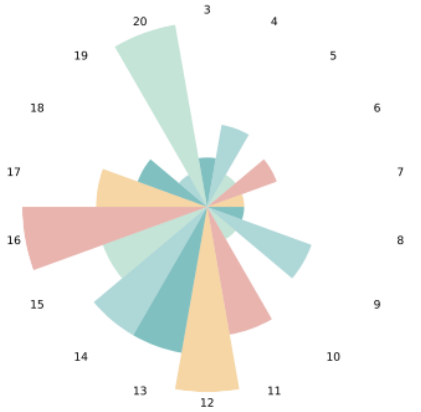
Vælg system

23 besvarelser fundet

Hent rapport

Kommune(demo) **SYSTEMEJERE**

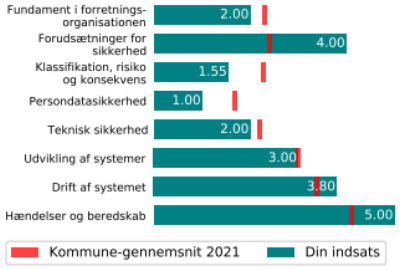
Status for de afgivne svar ift. KL's opgaveliste for sikkerhedsopgaver



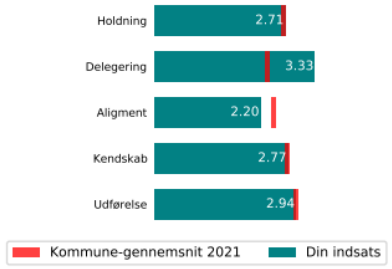
Data til denne rapport er fra din besvarelse af KL's baseline for sikkerhed i organisationen. Hvis ikke alle spørgsmål er medtaget / besvaret – f.eks. hvis opgaverne løses andre steder i kommunen -vil grafen (hjulet) ovenfor have tomme områder. Af grafen ovenfor til højre fremgår din besvarelse i forhold til andre af din kommunes deltagere.

Din status ift. øvrige system- og dataejere i din organisation. Grøn er merindsats, rød mindre-indsats.

Ansvarsområder



Forudsætninger



Spørgsmål, der kræver særlig opmærksomhed

Tabellen viser de spørgsmål, hvor mangler udgør en særlig stor risiko for informationssikkerheden eller behandlingen af persondata.

Spørgsmål	2021	kommune-gennemsnit	Vedrører
Har du sikret at databehandleraftalerne for dine systemer medtager de krav, som risikovurderingerne tilsiger?	1.0	2.0	Udførelse, Persondatasikkerhed
Har du sikret at de registreredes rettigheder til enhver tid kan imødekommes på dine systemer?	1.0	2.0	Udførelse, Persondatasikkerhed
Er der rutiner for dine systemer, så ændringer i systemkonfigurationer foregår planlagt og aftestet?	2.0	2.5	Udførelse, Teknisk sikkerhed
Kender du organisationens procedure for godkendelse af nye og ændrede it-systemer inden idriftsættelse?	2.0	2.5	Udførelse, Teknisk sikkerhed
Er ansvar og opgaver ifm. administration af brugeres systemadgang og rettigheder efter din mening klart defineret?	2.0	2.0	Holdning, Drift af systemet

Alle undersøgelsens spørgsmål er vurderet for om manglende implementering har direkte indflydelse på informationssikkerheden, beskyttelsen af følsomme personoplysninger eller udgør en risiko ifm. behandling af almindelige personoplysninger og personoplysninger om fx personale.

I-TRUST Denne rapport er automatisk genereret. I-Trust kan ikke holdes ansvarlig for beskrivelser, beregninger eller fremstillinger af informationer i denne rapport. Ved spørgsmål kontakt I-Trust på info@i-trust.dk.
Printet 04-11-2021
KL

KOMMUNE (DEMO)

Kommune (demo)	**KFE-risikoanalyse**
IT-risikoanalyse af Kommunesystem, 2021	Dato: 04-11-2021 Af: Kristian Bering Asmussen Sag/journal nr.: 12345678

Resultat af risikoanalyse

Skemaet giver et overblik over sandsynligheden for brud på it-sikkerheden og dermed persondatasikkerheden. Der er i skemaet ikke taget væsentligt hensyn til de data, der er i systemet, og konsekvensen ved brud på sikkerheden kan derfor ændre sig ved behandlingstyperne.

I denne risikoanalyse måles der på en score mellem 0 og 100, hvor 0 er laveste trussel, og 100 er højeste trussel. Alt under 35 vurderes til at være lav risiko.

Område	Kendskab	Forståelse	Efterlevelse
Governance - indeks	46	46	32
Leder -indeks	10	10	10
Adfærd - indeks	34	26	30
Kompetence - indeks	18	14	34
Hændelses/rapportering	45	45	66
Behandlingssikkerhed	35		
SUM	34	35	34

10 største individuelle risici

Det vurderes i denne rapport at der samlet set er middelhøje trusler

1. **Stilles der krav til brugernavn og adgangskode?**
2. **Anvendes deny list over ip-adresser?**
3. **Stilles der krav til brugernavn og adgangskode?**
4. **Tillades tidligere anvendte kodeord?**

Afslutning

KFE metoden

- Sikkerhedsarbejdet:
  - Kontroller
  - Awareness-skabende
  - Risikostyring ift. ansatte

- Organisationen
  - Redskab til organisationsprocesser – indførelse af roller, opgaver og ansvar
  - Målrettede sikkerhedsindsatser
    - Kendskab
    - Accept og opmærksomheder
    - Kompetencer

Spørgsmål?

Læs mere på:
www.i-trust.dk
Eller ring:
88626400