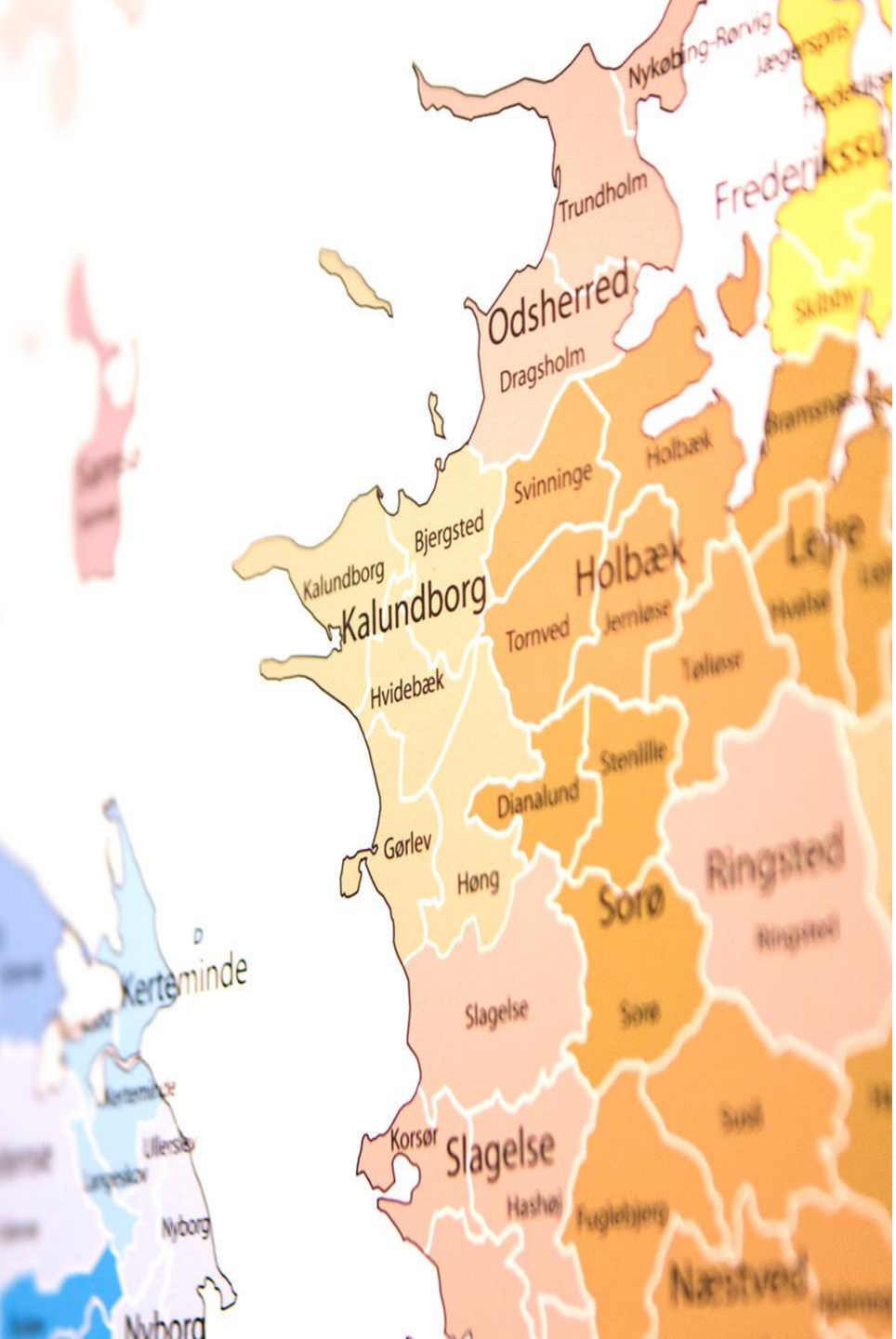
NSIS I KOMMUNERNE OG I FÆLLES LØSNINGER

Arkitekturrådsmødet 27. august 2019 /v Lars Vraa

KOMB:T
Kommunernes it-fællesskab



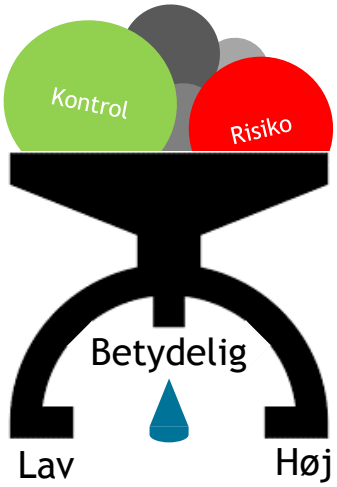
Agenda

- **Baggrund og introduktion til NSIS**
- **Betydning for kommunerne**
- **KOMBITs NSIS værktøj (under udvikling)**

KOMBIT
Kommunernes it-fællesskab

Helt overordnet… Hvad er NSIS

(NSIS - National Standard for Identiteters Sikringsniveauer)

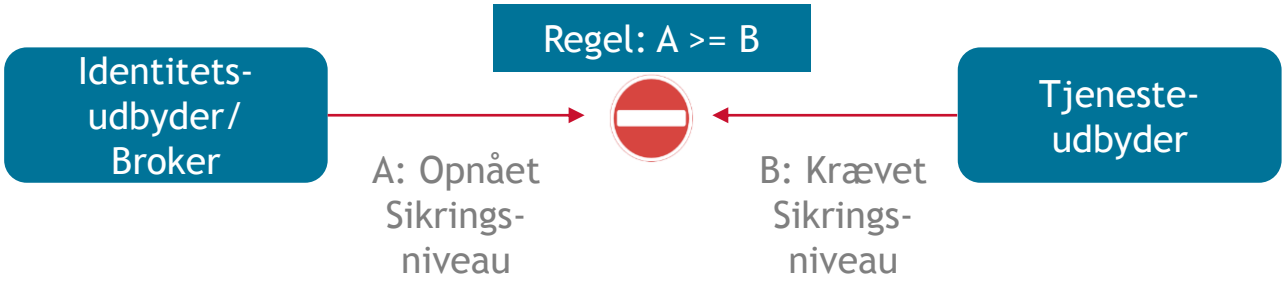


NSIS er et tillidsrammeværk og en national standard for digitale identiteter udgivet af Digitaliseringsstyrelsen, støttet af KL og regionerne.

NSIS handler om identiteter i føderationer, hvor én part udbyder en identitet (Identity Provider) og en anden part aftager identitet (Service Provider eller tjenesteudbyder).

Overholdelse af NSIS vedrører både organisatoriske, procesmæssige og tekniske aspekter.

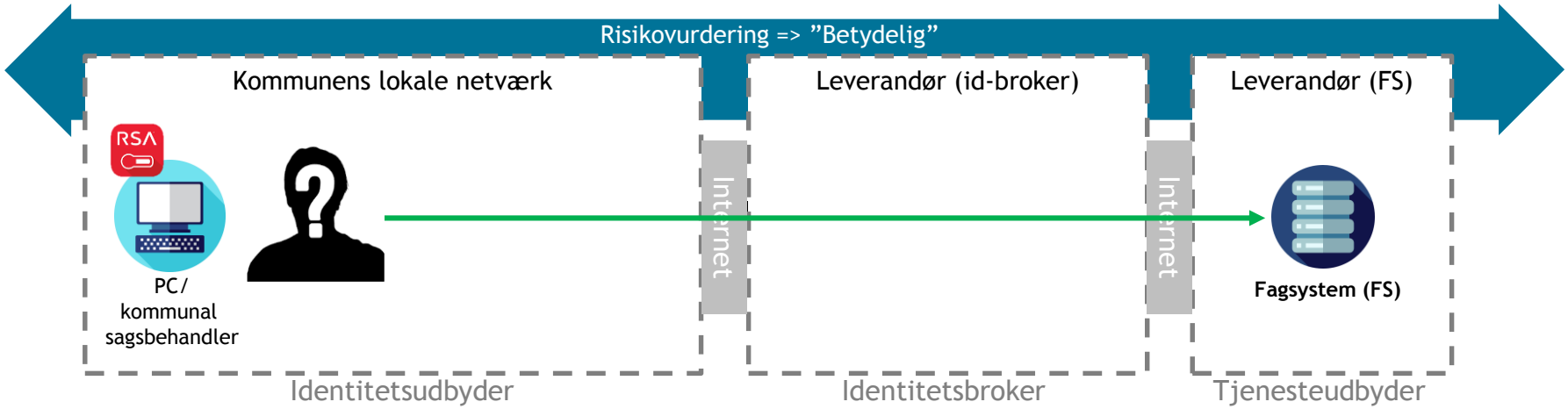
NSIS introducerer tre sikringsniveauer; lav, betydelig og høj. Hvilket niveau, der kræves for en læsning, tager afsæt i en risikovurdering



Vigtige ressourcer: https://www.digitaliser.dk/resource/4397607

KOMBIT
Kommunernes it-fællesskab

Eksempel, fælleskommunalt fagsystem hvor adgangsstyring sker via 3.part over Internettet



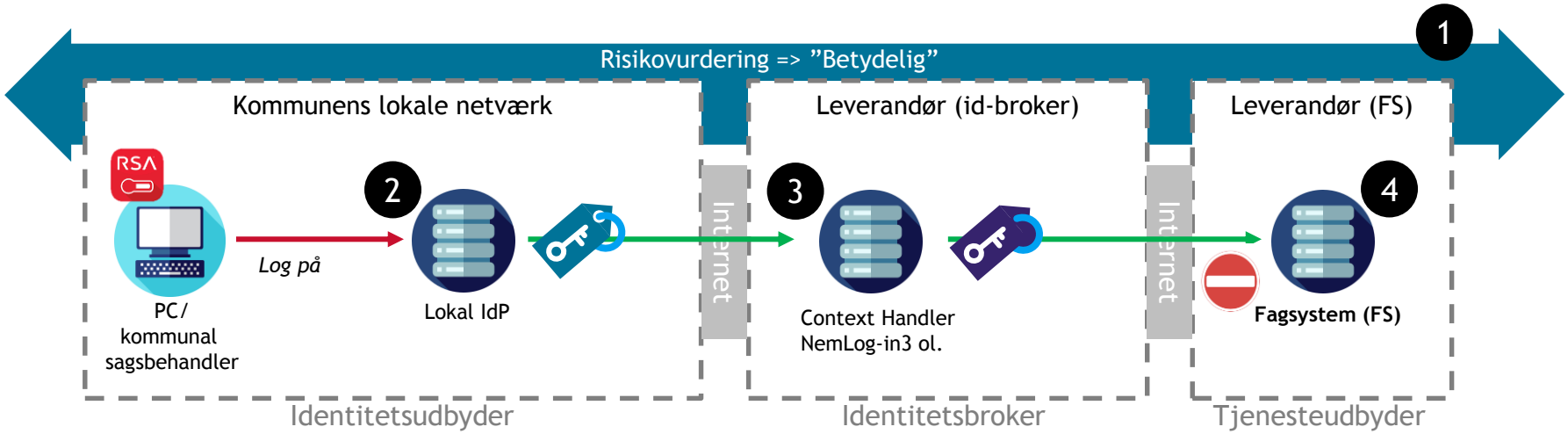
Hvordan kan tjenesteudbyder stole på identitet som modtages via 3.part over internettet?

Hvordan stilles der krav som alle parter kan forstå og enes om?

Det er det NSIS giver et bud på…

KOMBIT
Kommunernes it-fællesskab

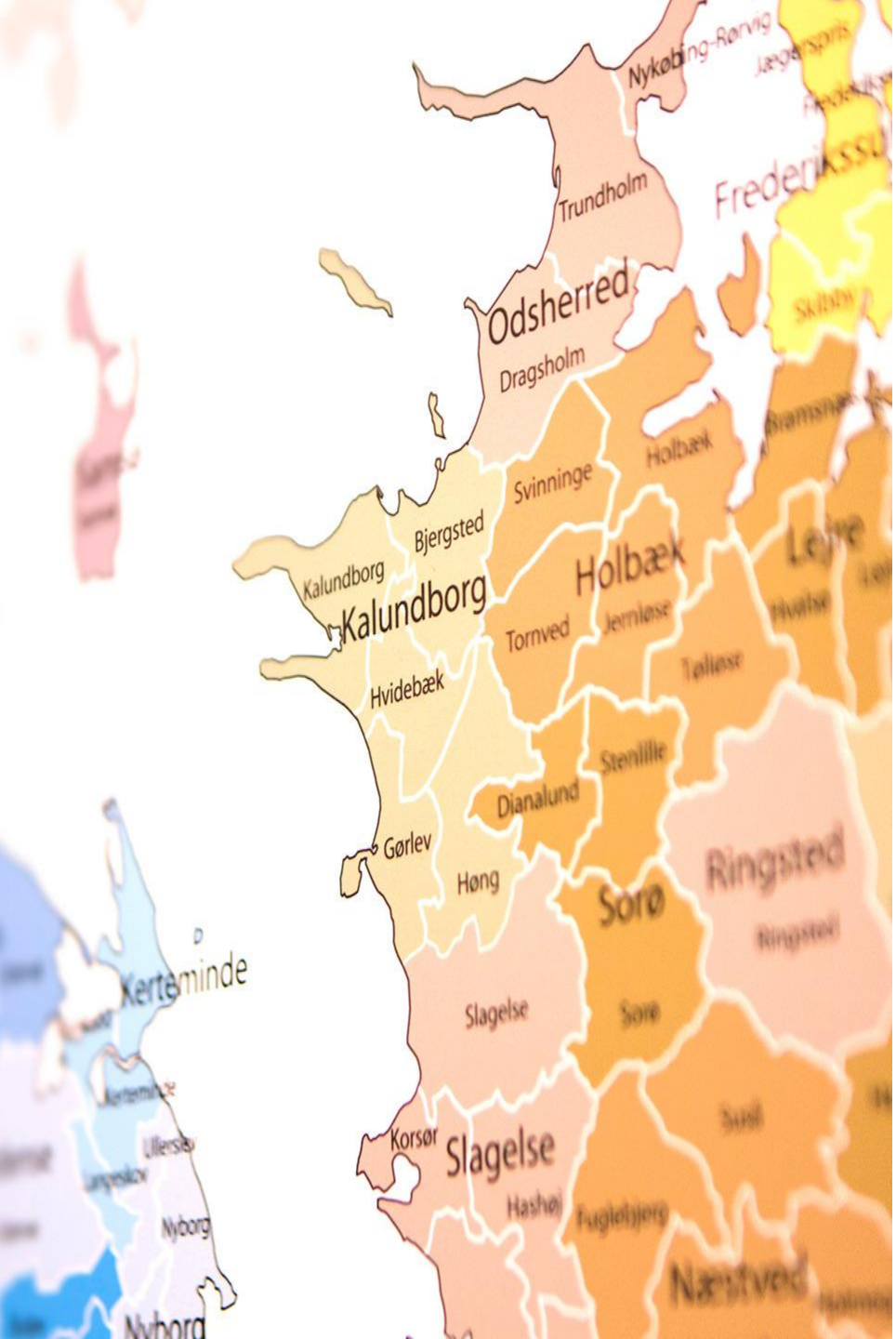
Eksempel, fælleskommunalt fagsystem hvor adgangsstyring sker via 3.part over Internettet



Fastsættelse af Sikringsniveau og overholdelse:

1) IT-systems sikringsniveau fastsættes på baggrund af helhedsorienteret sikkerhedsvurdering per brugertype. Fx Betydelig.
2) Bruger logger på lokalt i kommunen. IdP udsteder token hvor sikringsniveau indgår.
3) Bruger sendes videre til broker fx context handler. Ny token udstedes.
4) Sikringsniveau indgår i token og verificeres af IT-system. Dvs. er opnået >= krævet sikringsniveau.

KOMBIT
Kommunernes it-fællesskab

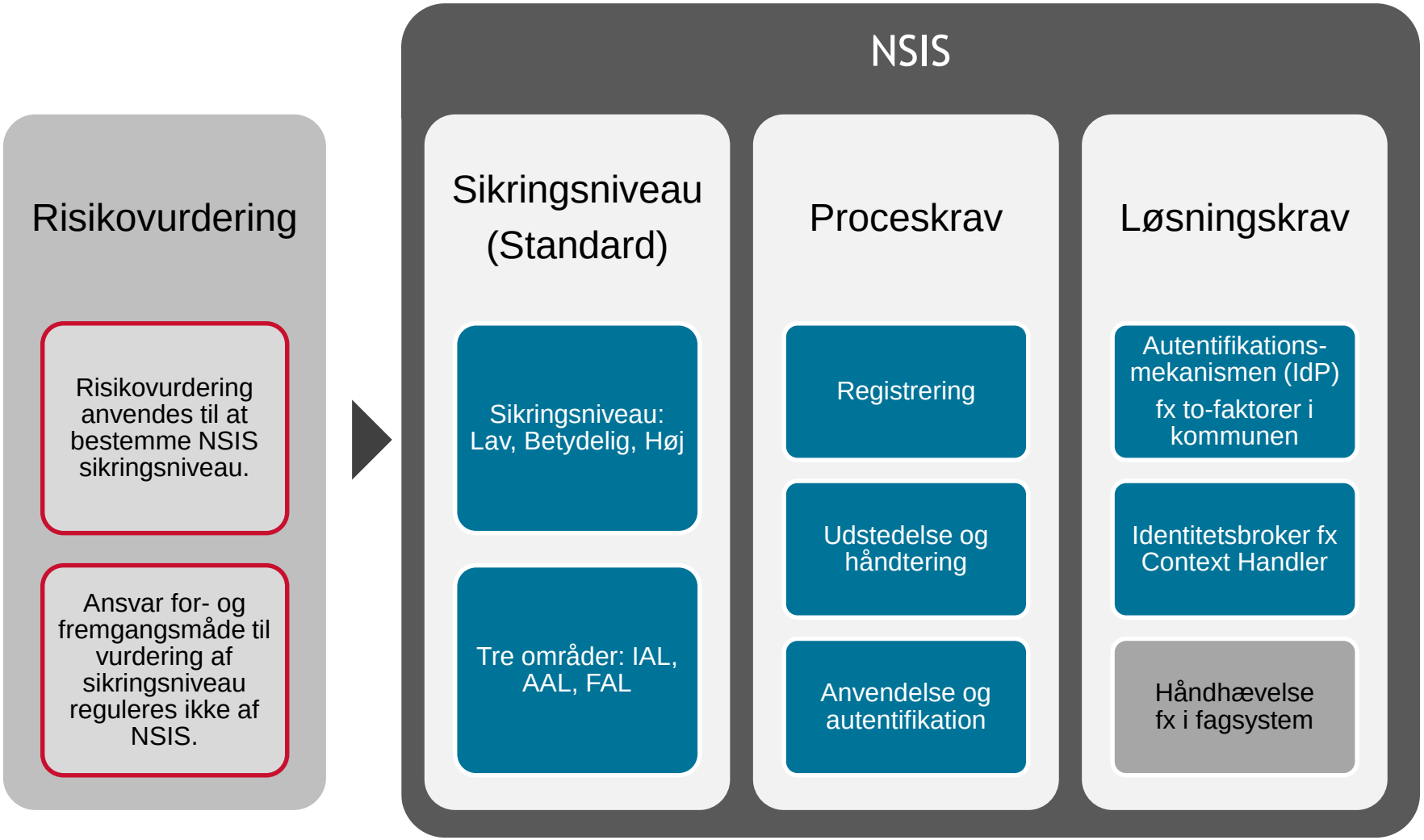


Agenda

- **Baggrund og introduktion til NSIS**
- **Betydning for kommunerne**
- **KOMBITs NSIS værktøj (under udvikling)**

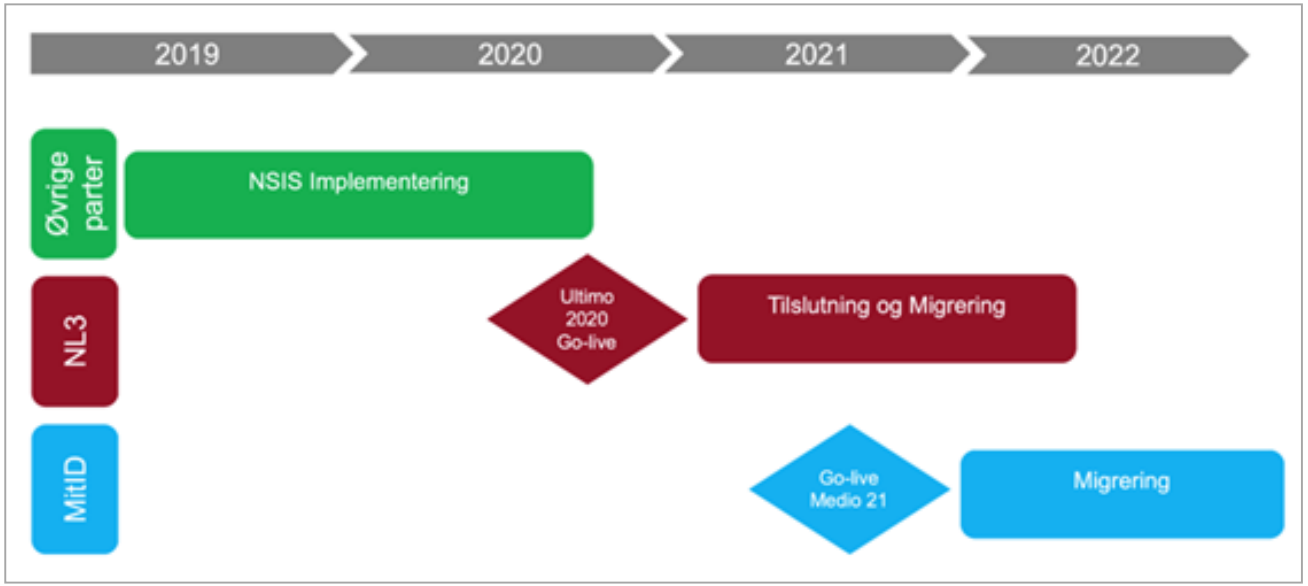
KOMBIT
Kommunernes it-fællesskab

Væsentlige elementer i NSIS



KOMBIT
Kommunernes it-fællesskab

Hvornår skal NSIS overholdes? Konsekvenser?

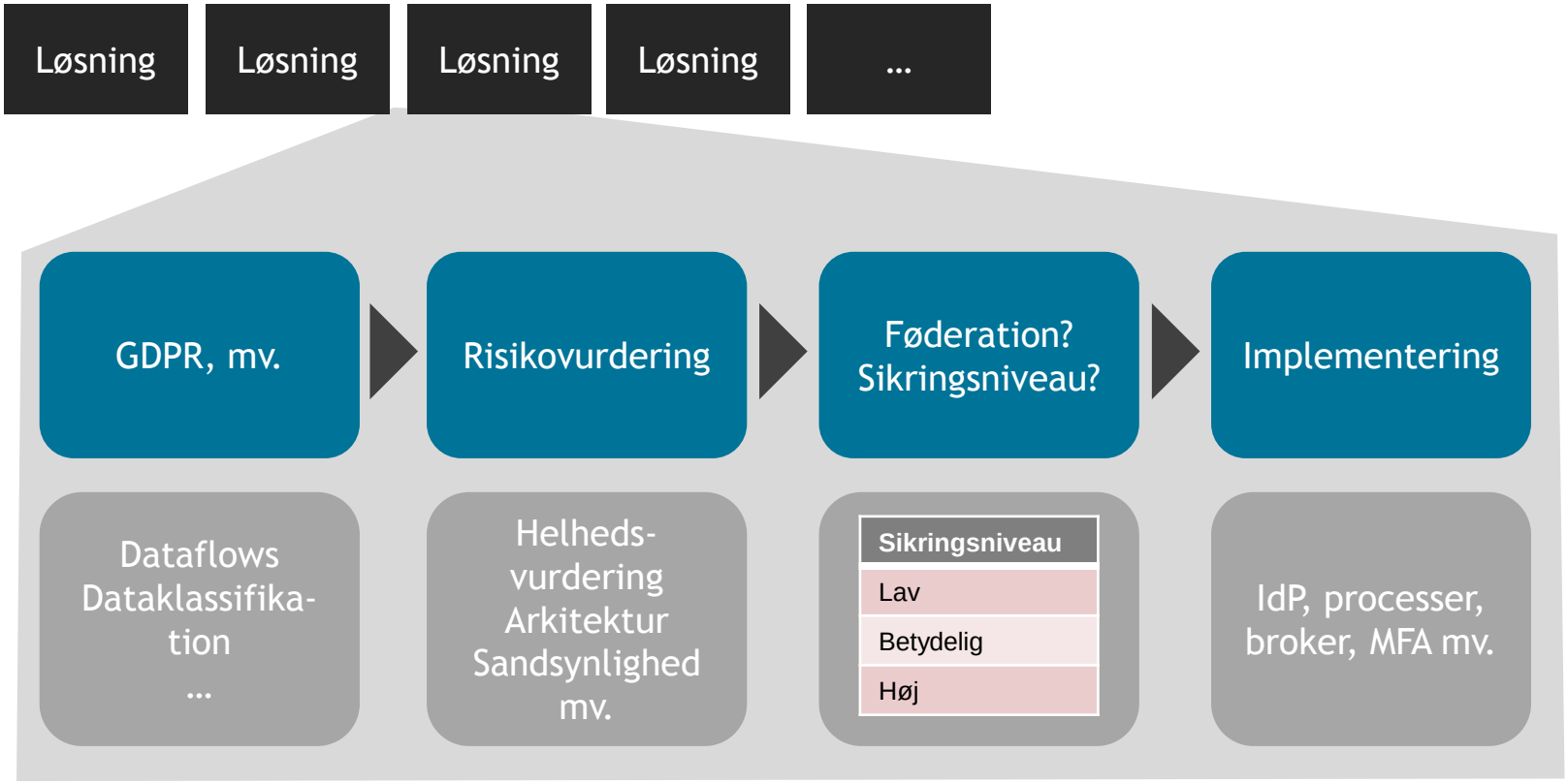


- Ny plan fra DIGST viser at staten først fuldt ud overholder NSIS ultimo 2020…
- KOMBIT har implementeret NSIS i fælleskommunale løsninger og kræver rent teknisk at sikringsniveau er sat i tokens, AULA, SAPA mv.
- NSIS overholdelse bliver en forudsætning for at anvende MitID og Nemlog-in3 fuldt ud i kommunerne.
- DIGST vil fra ultimo 2020 stille krav om revisorerklæringer som dokumenterer NSIS overholdelse.

https://digst.dk/it-loesninger/implementeringssite/screeningsvaerktoej-til-brugerorganisationer-og-tjenesteudbydere/nsis-ibrugtagning-af-standarden/

KOMBIT
Kommunernes it-fællesskab

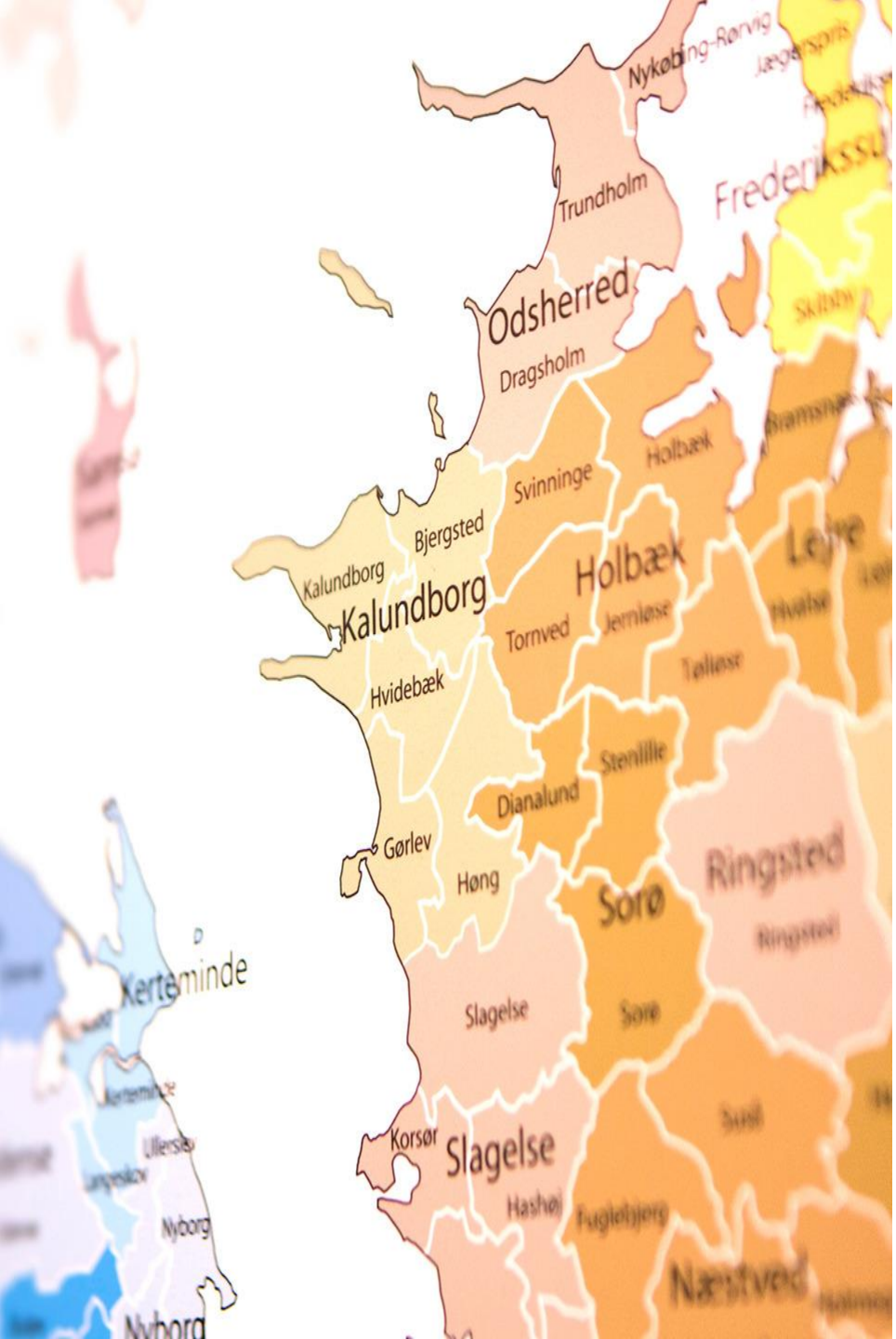
Fastsættelse af sikringsniveau og implementering



NSIS vurdering bør indgå som del af kommunens øvrige sikkerhedsarbejde
Kan blive en større opgave i takt med brugen af føderation stiger.

Udfordring at fastsætte passende og så vidt muligt ensartet niveau på tværs af kommuner, myndigheder mv. for tilsvarende løsninger

KOMBIT
Kommunernes it-fællesskab



Agenda

- **Baggrund og introduktion til NSIS**
- **Betydning for kommuner**
- **KOMBITs NSIS værktøj (under udvikling)**

KOMBIT
Kommunernes it-fællesskab

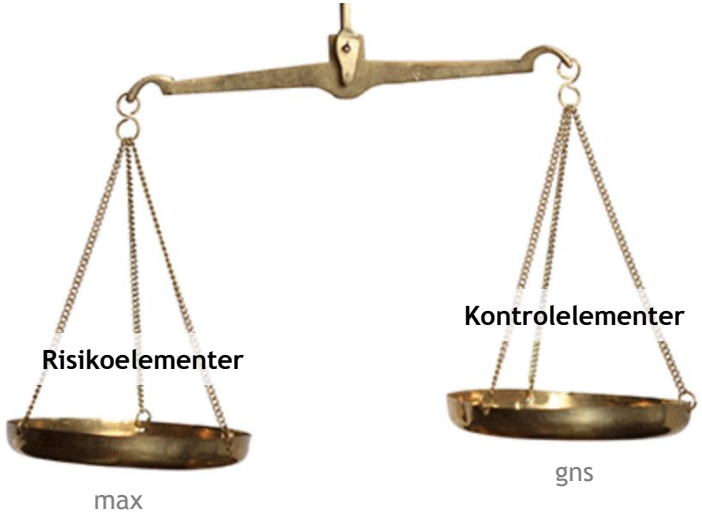
Metodik for NSIS-vurdering - *balanceret* tilgang

Integreret del af GDPR-proces. Analyser og dokumentation af data kan genbruges.

For hver brugertype i systemet afdækkes:

- **Risikoelementer** som kan føre til risici relateret til eksterne identiteter (uønskede konsekvenser for KOMBIT, kommuner og de registrerede).
- **Kontrolelementer** som mitigerer risici relateret til eksterne identiteter

Det samlede sikringsniveau for en brugertype findes ved at sammenholde risiko- og kontrolelementer på en balanceret måde.



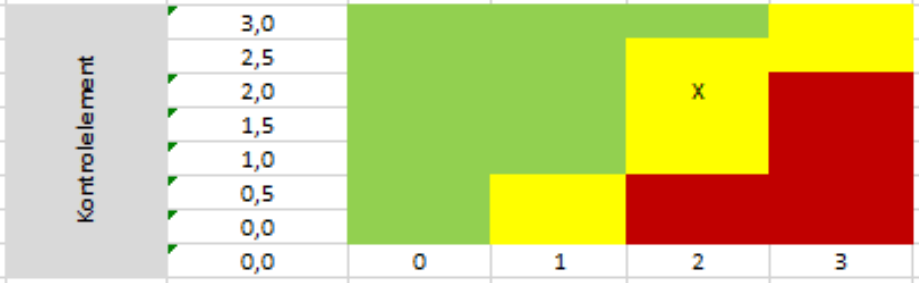
KOMBIT
Kommunernes it-fællesskab

Samlet vurdering og fastsættelse af sikringsniveau

Projekt / system	SAPA
Projektleder	Anders Cronwald
Projektetsfase	
Brugertype	Sagsbehandler

Assessor	TRI, LVR, TG, RHI
Assessment dato	1. juni 2019

Score risikoelementer (max)	2,0
Score kontrolelementer (gennemsnit)	2,1
Samlet vurdering af sikringsniveau	Betydelig



Farvekode for kombinationen:	NSIS Niveau Lav
	NSIS Niveau Betydelig
	NSIS Niveau Høj

KOMBIT
Kommunernes it-fællesskab

BACKUP

KOMBIT
Kommunernes it-fællesskab

Risikoelementer

Risikoelementer	Score (1-3)	Angiv begrundelse for score		Indikator for sikrings
A. Brugertypens adgang til personoplysninger	2	SAPA fremviser oplysninger om sygehusindlæggelser og arbejdsskader samt oplysninger fra cpr-registeret. Adgangen til cpr-oplysninger kan rettighedsstyres til enten at ske pr. kommune eller på landsplan; mens oplysninger om sygehusindlæggelser og arbejdsskader er opdelt pr. kommune NB. Opslag i cpr-registeret på et ændret cpr-nummer vil give oplysninger op borgerens nye cpr-nummer	1. Lav 2. Betydelig 3. Høj	Ingen eller meget begræns Bemærk at CPR-numre ik Adgang til følsomme pers Adgang til store mængder landsdækkende etc). Et ek sundhedsoplysninger.
B. Brugertypens adgang til øvrige typer oplysninger	1	Ingen forretningsdata i SAPA	1. Lav 2. Betydelig 3. Høj	Ingen eller meget begræns Adgang til en vis mængde Adgang til store mængder
C. Konsekvenser for registrerede ved at forkert identitet under brugertypen tilgår systemet inkl. deres data	2	Der vil kunne lækkes sundhedsoplysninger og oplysninger fra cpr-registeret	1. Lav 2. Betydelig 3. Høj	Mindre alvorligt for registr Alvorligt for registrerede - Ødelæggende - mulighed f handlefrihed
D. Konsekvenser for KOMBIT/kommune ved at forkert identitet under brugertypen tilgår systemet inkl. deres data (fortrolighed)	2	Bøder fra datatilsynet kan næppe udelukkes ej heller en midlertidig nedlukning af systemet; men et læk af data fra SAPA er ikke så ekceptionel en hændelse at det vil være ødelæggende for KOMBIT eller kommunerne	1. Lav 2. Betydelig 3. Høj	Mindre alvorligt for KOME Alvorlige konsekvenser fo kommuner, pressesager m Ødelæggende hændelse fo
E. Brugertypens mulighed for at påvirke integritet for systemets eller data (herunder ændre/smadre data eller opførsel)			1. Lav 2. Betydelig 3. Høj	Ubetydelig mulighed for at tilstrækkeligt. En vis mulighed for at ænd retableres inden for 24-48 Mulighed for at ændre stø ændre systemet væsentlig Systemet er vitalt for kom
F. Brugertypens mulighed for at påvirke tilgængelighed for system eller data (herunder slette data eller smadre systemet)			1. Lav 2. Betydelig 3. Høj	Ubetydelig mulighed for at tilstrækkeligt. En vis mulighed for at slett retableres inden for 24-48 Mulighed for at slette stø stoppe systemet i en lang
	Maksimum 2,0			

KOMBIT
Kommunernes it-fællesskab

Kontrolelementer

Område	Rationale for kontrolområde	Score (1-3)	Angiv begrundelse for score	Indikato
A. Adgangskontrol og rolledesign	En stærk adgangskontrol begrænser muligheden for at elevere brugeradgang til et højere sikringsniveau, hvis differentieret adgang med forskellige sikringsniveauer eksempelvis tillades. Et finkornet rolledesign giver mulighed for at afgrænse brugernes adgang i overensstemmelse med deres arbejdsbetingede behov, så eksponeringen reduceres.	2	SAPA giver kommunerne en finkornet mulighed for at begrænse brugerne adgang på grundlag af roller og dataafgrænsninger	1. Lav styr 2. Betydel 3. Høj styr
B. Robusthed, test og assurance	Jo bedre applikationens identitetshåndtering er verificeret og testet, jo mindre risiko er der for, at den fejler eller kan omgås.	3	F-Secure har gennemført en sikkerhedstest af SAPA og alle alvorlige anmærkninger er efterfølgende mitigeret	1. Lav styr 2. Betydel 3. Høj styr
C. Logning og overvågning	En god logning og overvågning gør det muligt at detektere fejl, angreb og anomalier og derved at begrænse skadens omfang gennem passende reaktion. Der er mao. tale om en reaktiv kontrol og ikke en forebyggende.	2	Brugeradgange logges konsekvent. Kommunerne har adgang til logning og kan gennemføre kontrol og opfølgning.	1. Lav styr 2. Betydel 3. Høj styr
D. Vejledninger og instruks til kommuner	Jo bedre kommuner og andre anvendere forstår at opsætte brugeradgange og anvende systemets funktionalitet til brugerstyring, jo mere reduceres risikoen for fejlopsætning.	2	Brugeradgange er udførligt beskrevet i dokumentationen. KL har forfattet notat med anbefalinger ud fra en juridisk vinkel Alle kommuner vil deltage/har deltaget i administratorkurser, hvor opsætning af brugeradgange behandles KOMBIT har udfærdiget vejledning og faciliteret videndeling om opsætning af jobfunktionsroller mv.	1. Lav styr 2. Betydel 3. Høj styr
E. Funktionsadskillelse	Funktionsadskillelse reducerer risikoen for, at en bruger alene kan foretage kritiske handlinger, så eksempelvis to forskellige brugeridentiteter skal kompromitteres, før alvorlige konsekvenser udløses.	2	Forskellige opgaver i SAPA er beskyttet af forskellige brugersystemroller SAPA har ikke implementeret logik, der blokerer for at en bruger kan udføre alle typer af opgaver i systemet.	1. Lav styr 2. Betydel 3. Høj styr
F. Sikre forbindelser	Sikre forbindelser og standardiserede føderationsprotokoller mitigerer tekniske risici forbundet med, at en brugeridentitet overdrages fra en identitetsudbyder (IdP) til en tjenesteudbyder (forretningsapplikation).	2	SAPA følger de anbefalinger som er givet af F-Secure i forbindelse med sikkerhedstesten af systemet med enkelte undtagelser for interne forbindelser hos driftsleverandøren	1. Lav styr 2. Betydel 3. Høj styr
G. Kontrol med brugersessioner	Hvis en brugersession kan overtages, kan en legitim brugeridentitet misbruges.	2	Der er implementeret timeout for brugersessioner, Session cookies er beskyttet af httpOnly- og secure-flagene. SAPA er beskyttet mod CSRF.	1. Lav styr 2. Betydel 3. Høj styr
Se alene på kontroller som mitigerer sandsynlighed eller konsekvens af forkert identitet		**Gennemsnit 2,1**		

KOMBIT
Kommunernes it-fællesskab

Emner til drøftelse

Overholdelse af NSIS

- I hvilken grad og hvornår er kommunerne forpligtet til at følge NSIS? Hvad er konsekvenserne hvis NSIS implementeres delvist og gradvist?
- Hvilken fremgangsmåde og værktøjer skal vi anvende til at udføre og dokumentere risikovurderinger for kommunale IT-systemer og infrastruktur?
- Hvordan fastsætter et passende og så vidt muligt ensartet niveau, både kommunerne imellem, men også ift. andre sektorer.
- Fremtidsudsigter, kan vi påvirke kommende versioner af NSIS?

Erfaringsudveksling

- Findes der løsninger og erfaringer i kommunerne fx ift. effektiv to-faktor login som kan deles og eventuelt genbruges?
- Hvordan defineres et korrekt to-faktor login, og hvor længe vil det kunne gælde før der skal kræves nyt login?

KOMBIT
Kommunernes it-fællesskab

Øvrige emner og spørgsmål

Udfordringer for kommunerne, KL og KOMBIT

- Spring fra lav til betydelig er meget markant
- Organisatoriske og procesmæssige krav fx ved registrering og udstedelse af logins
- Registrere kommunal IdP hos Digitaliseringsstyrelsen
- Årlig revisionsrapport fra en statsautoriseret revisor
- Udføre egenkontroller mellemliggende periode
- Specifikke krav om at kunne fravælge single sign-on og begrænse tokens til specifikke tjenester
- Uklar definition af national broker

Udbredelse

- Tidsplan for implementering nationalt
- National infrastruktur forventes ikke at overholde NSIS før 2020+
- Dialog med STIL om NSIS på skoleområdet og forslag om alternativ standard

KOMBIT
Kommunernes it-fællesskab