Digdir

digdir.no

Felles sikkerhet i forvaltningen

-

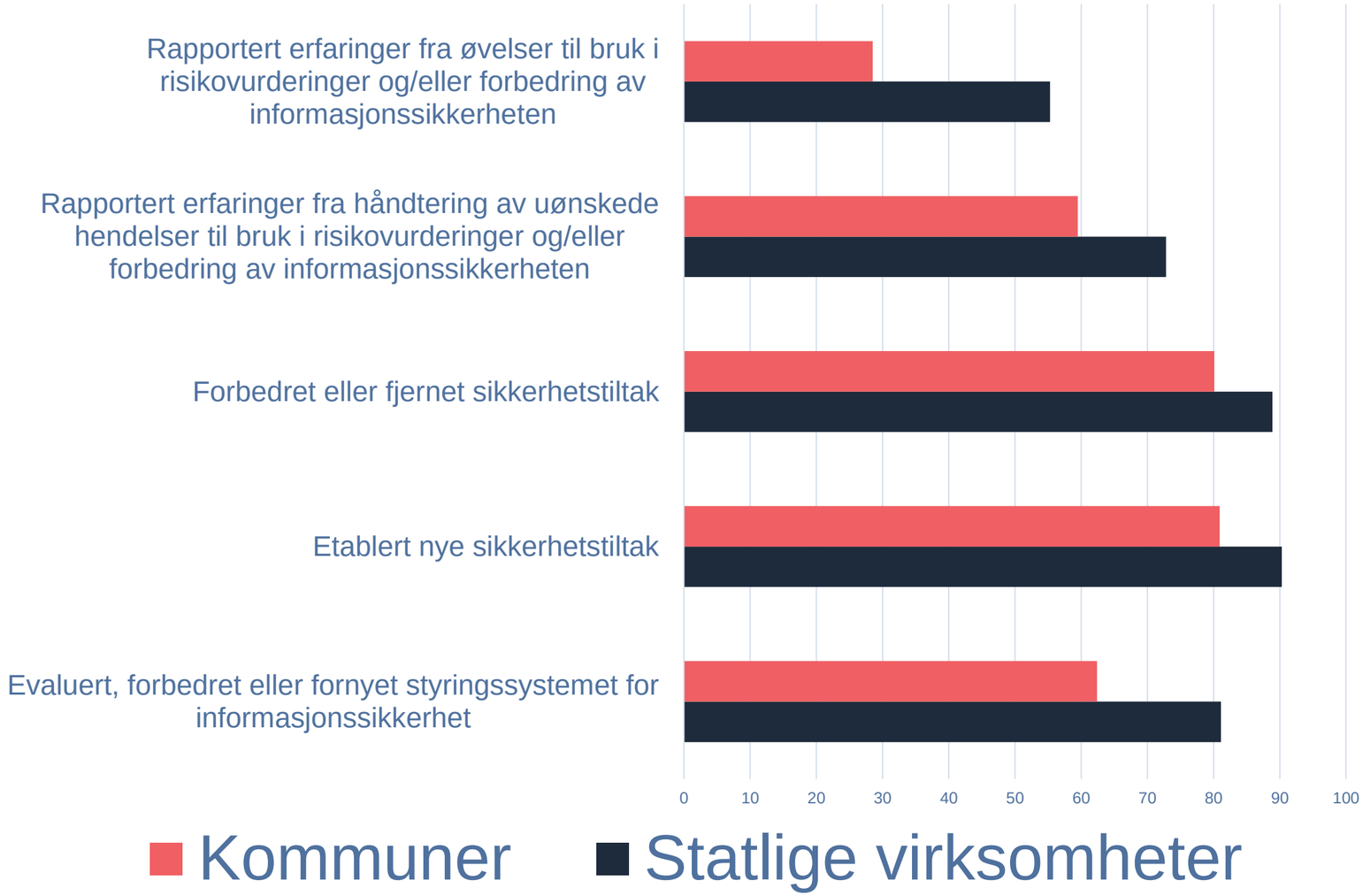
NIFS-møte 14. september 2022

Agenda

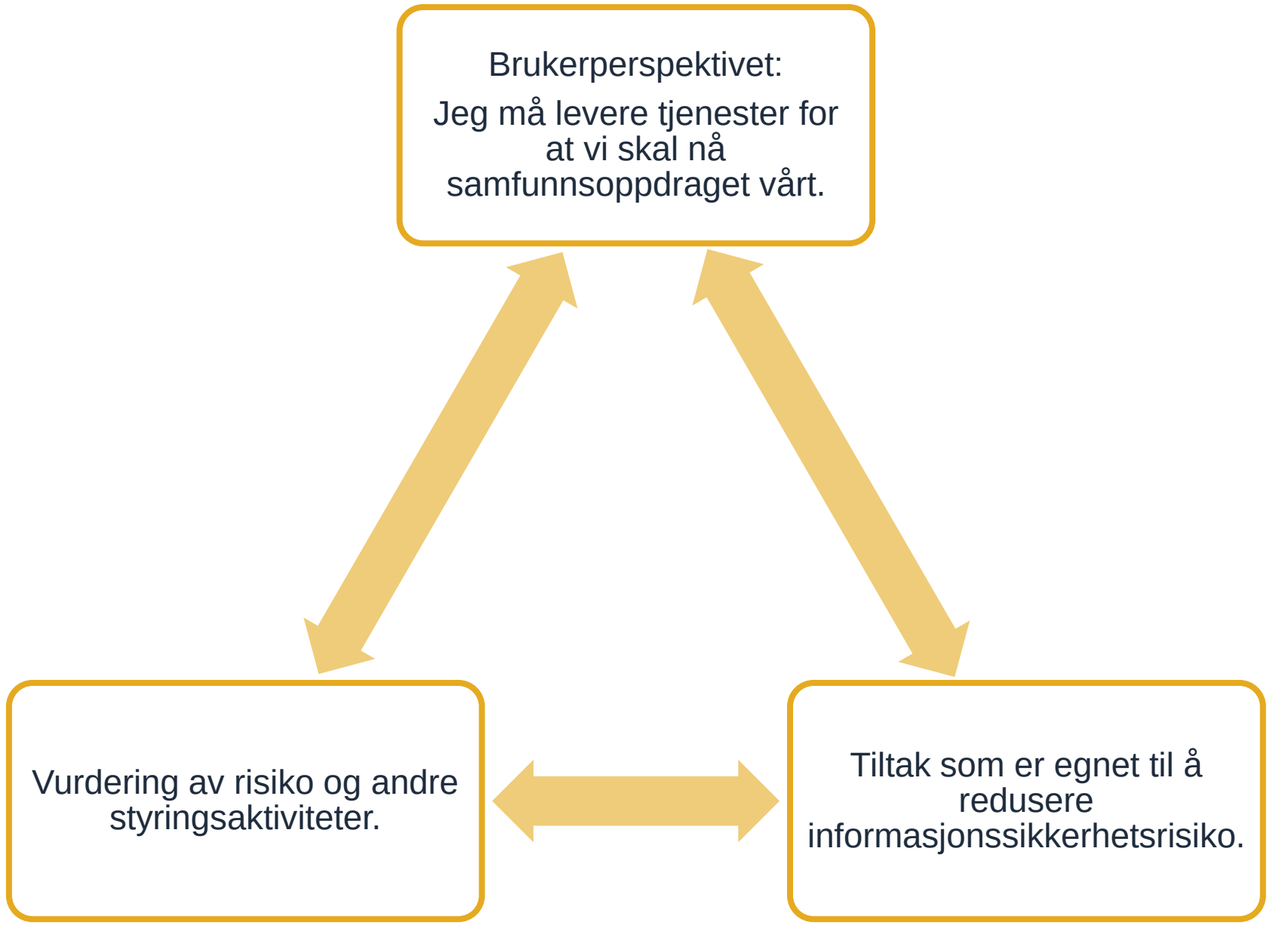
1. Bakgrunn
2. Hvorfor felles sikkerhet i forvaltningen?
3. Hvordan kan det gjøres?

Bakgrunn

Utfordringsbildet



Virksomhetsperspektivet



Digdir

digdir.no

«Felles sikkerhet i forvaltningen»

Viktige spørsmål virksomhetene må stille seg selv.

Hvilke oppgaver leverer vi, og hvilken informasjon behandles?

Hvor store konsekvenser kan informasjonssikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?

Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave

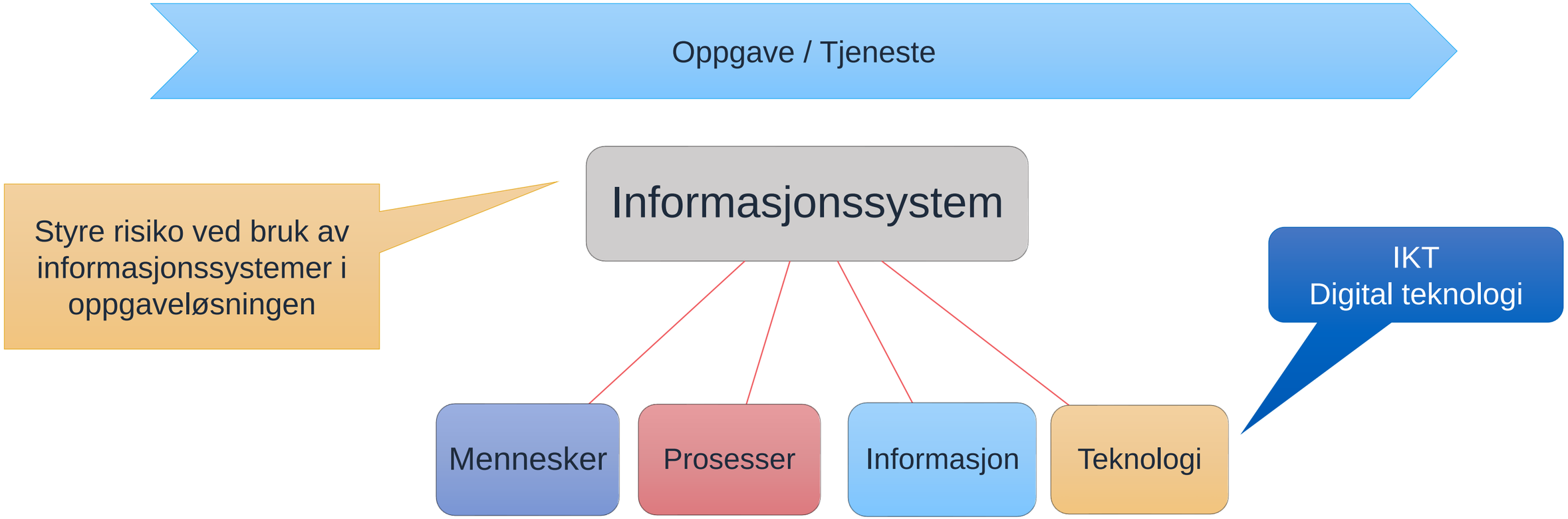
Anbefalte minimumstiltak

Svar fra veiledningsaktørene, på ett sted, felles for alle.

Felles sikkerhet i forvaltningen

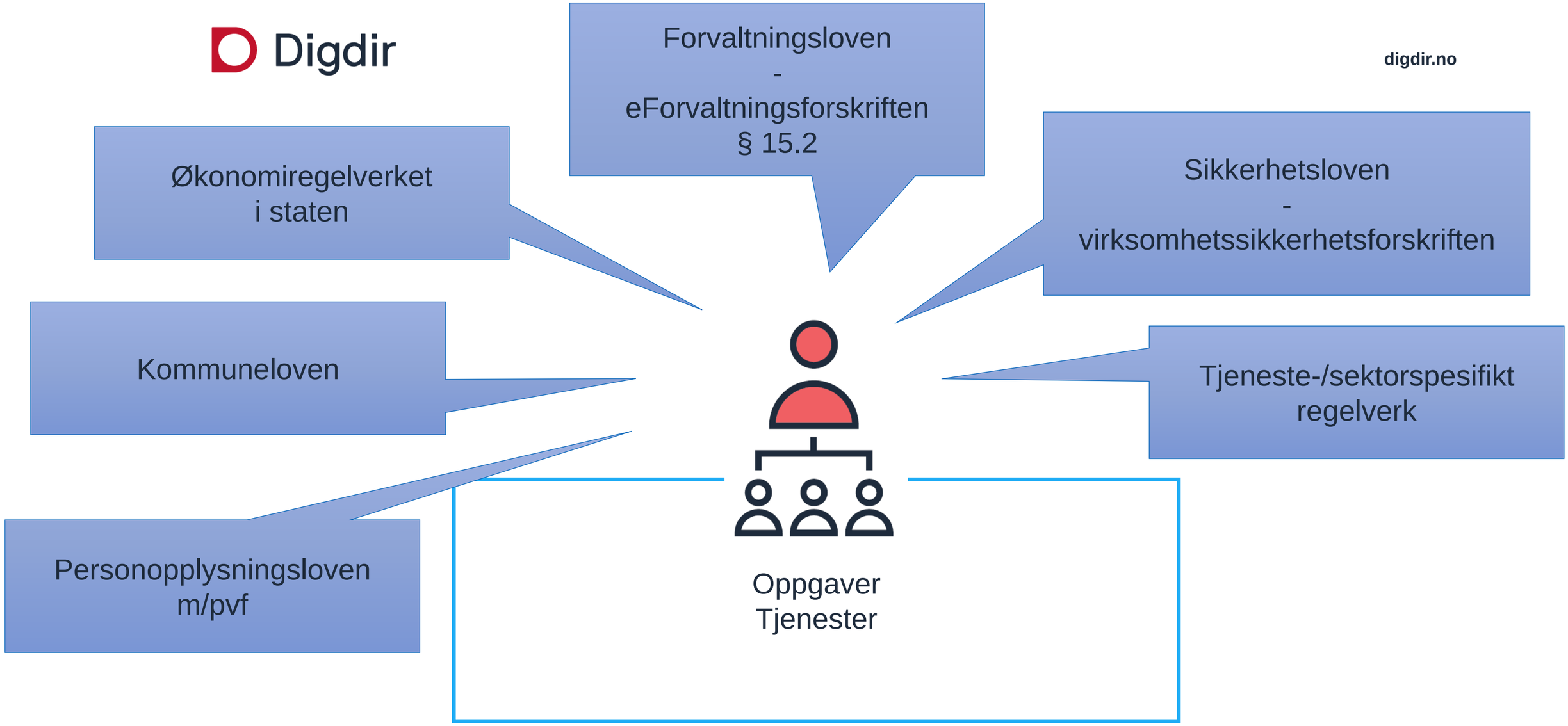
- Et initiativ fra Digitaliseringsdirektoratet
- Konkret veiledning - brukerorientert
- Gjøre like ting likt
- Samarbeid mellom veiledningsaktørene
- Notat – utgangspunkt for videre arbeid

Hvorfor?


Oppgave / Tjeneste
Informasjonssystem
Styre risiko ved bruk av informasjonssystemer i oppgaveløsningen
IKT
Digital teknologi
Mennesker
Prosesser
Informasjon
Teknologi

Digdir

digdir.no



Selvstendig ansvar for styring og kontroll

Tilstrekkelig / Risikobasert

Redskap: risikostyring

Styringsaktiviteter

- Ledelsens styring og oppfølging
- Risikovurdering
- Risikohåndtering
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon

Sikkerhetstiltak

Formål

- Forebygge
- Oppdage
- Håndtere og gjenopprette

Typer

- Organisatoriske
- Menneskelige
- Fysiske
- Teknologiske

«Erfaring viser imidlertid at anbefalinger og veiledninger i varierende grad blir fulgt opp av virksomheter. Forståelsen for forebyggende digital sikkerhet er begrenset i mange virksomheter, ikke minst på ledelsesnivå.»

Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden, kapittel 8.2

Utredningen NOU 2018:14 viser at dagens regelverk er krevende å etterleve

NOU 2018:14 om IKT-sikkerhet viser at eksisterende funksjonsbaserte regelverk er krevende å etterleve og at mange virksomheter mangler tilstrekkelig kompetanse til å vurdere hva som ligger i regelverkets krav[1].

- **Mange har ikke tilstrekkelig kompetanse** til å etterleve funksjonsbaserte regelverk, og kravene er ofte overordnede og vage. For vage krav kan medføre dårligere etterlevelse på grunn av **usikkerhet rundt hva som kreves for å oppfylle kravet**.
- Funksjonsbaserte regelverk setter også **større krav til at virksomhetene har tilstrekkelig kompetanse** og evne til å vurdere hva som ligger innenfor regelverkets krav.
- Blir regelverket for generelt eller vagt, kan det gi store **variasjoner i etterlevelsen og håndhevingen**.

[1] IKT-sikkerhet i alle ledd - Organisering og regulering av nasjonal IKT-sikkerhet (NOU 2018:14)

Problembeskrivelser

Svake eller manglende styringsaktiviteter

Mangler grunnleggende sikkerhetstiltak

Utilstrekkelig oversikt over informasjonsbehandlingen

Må til en viss grad gjøre de samme vurderingene

Mangelfull forvaltning av sikkerhetstiltak

Kompetansekrevende

Ressurskrevende

Krevende å undersøke om omfang av sikkerhetstiltak er tilstrekkelig

Vanskelig å evaluere på tvers av virksomheter

Utfordrende å bruke og følge opp tjenesteleverandører

Manglende tillit mellom virksomheter kan være hinder for digitalisering

Vanskelig å få til en helhetlig tilnærming i virksomhetene

Mangelfull og fragmentert regulering

Problembeskrivelser

Svake eller manglende styringsaktiviteter

Mangler grunnleggende sikkerhetstiltak

Utilstrekkelig oversikt over informasjonsbehandlingen

Må til en viss grad gjøre de samme vurderingene

Mangelfull forvaltning av sikkerhetstiltak

Kompetansekrevende

Ressurskrevende

Krevende å undersøke om omfang av sikkerhetstiltak er tilstrekkelig

Vanskelig å evaluere på tvers av virksomheter

Utfordrende å bruke og følge opp tjenesteleverandører

Manglende tillit mellom virksomheter kan være hinder for digitalisering

Vanskelig å få til en helhetlig tilnærming i virksomhetene

Mangelfull og fragmentert regulering

Digdir

digdir.no

Hvordan kan det gjøres?

Hva om vi har…

Felles referanseramme

Mer helhetlig «rammeverk» av

- Regelverkskrav
- Anbefalinger
- Veiledning

Aktører som samarbeider og koordinerer i helheten

Eksempel fra hverdagen

Viktige spørsmål virksomhetene må stille seg selv.

Hvilke oppgaver leverer vi, og hvilken informasjon behandles?

Hvor store konsekvenser kan informasjons-sikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?

Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave

Anbefalte minimumstiltak

Svar fra veiledningsaktørene, på ett sted, felles for alle.

Digdir

digdir.no

Katalog med oppgaver og informasjonstyper

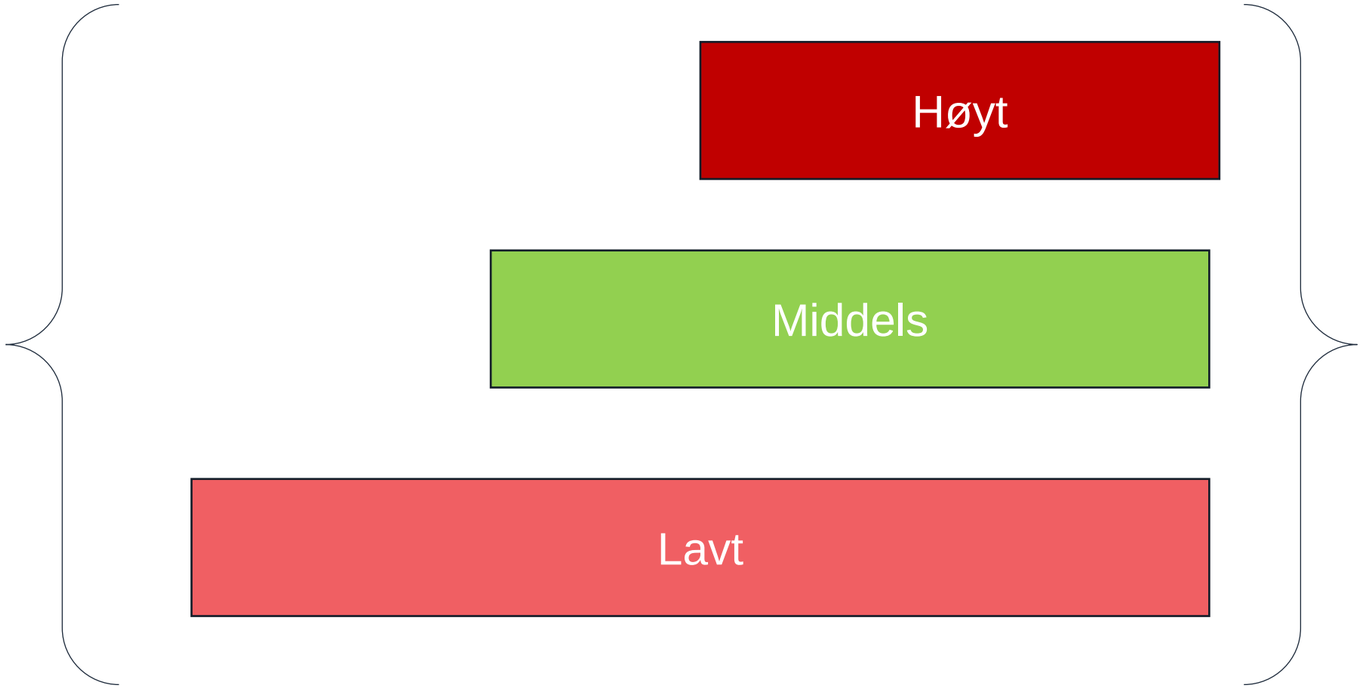

Offentlig forvaltning
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Mer felles
Gode rammebetingelser og hjelpemidler
(regelverk / anbefalinger / veiledning)

Digdir

digdir.no

Vurdering av konsekvensnivå per oppgave

Konsekvensnivåer



Digdir

digdir.no

Anbefalte minimumstiltak

Mange tiltaksbanker i bruk i forvaltningen

NIST

SP 800-53 r5

ISO/IEC

27002

NSM
IKT-sikkerhet

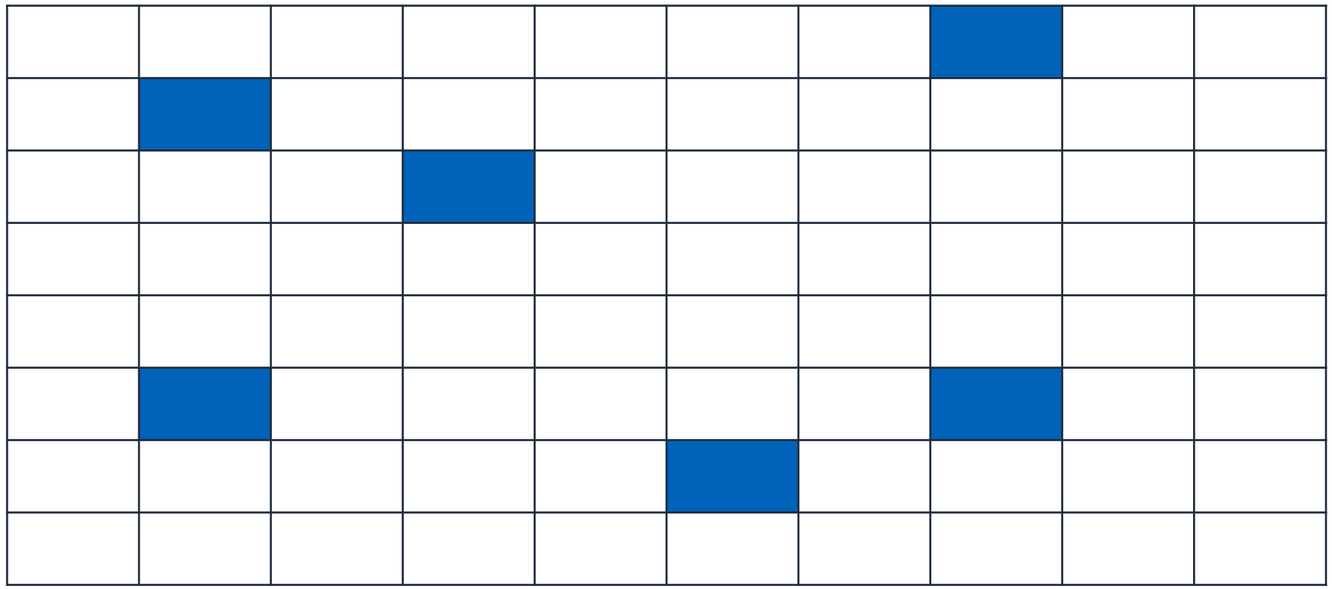
NSM
Fysisk sikkerhet

NSM
Personellsikkerhet

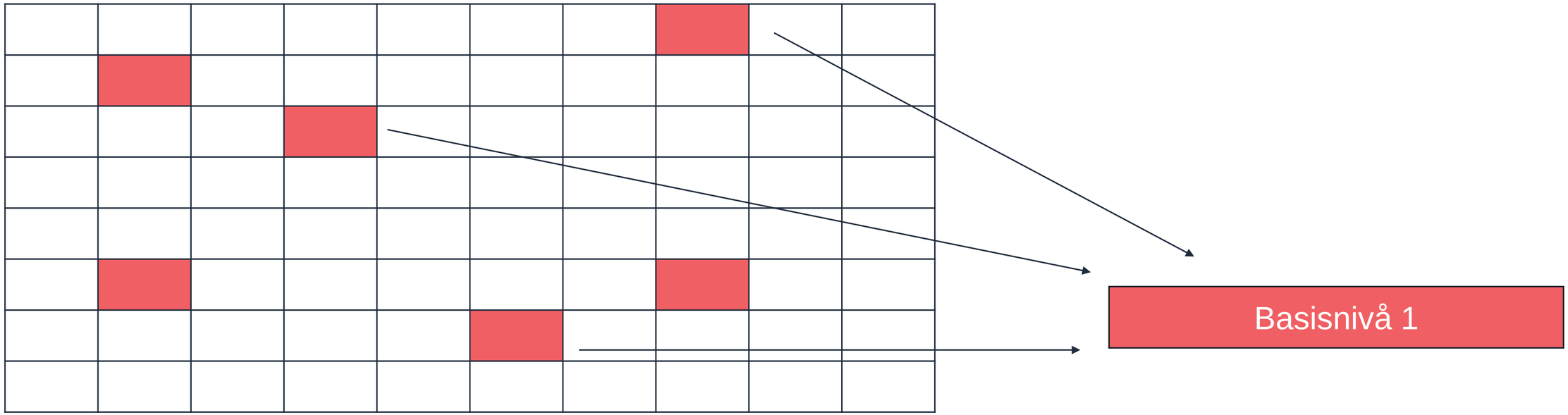
NIST

Cyber Security
Framework

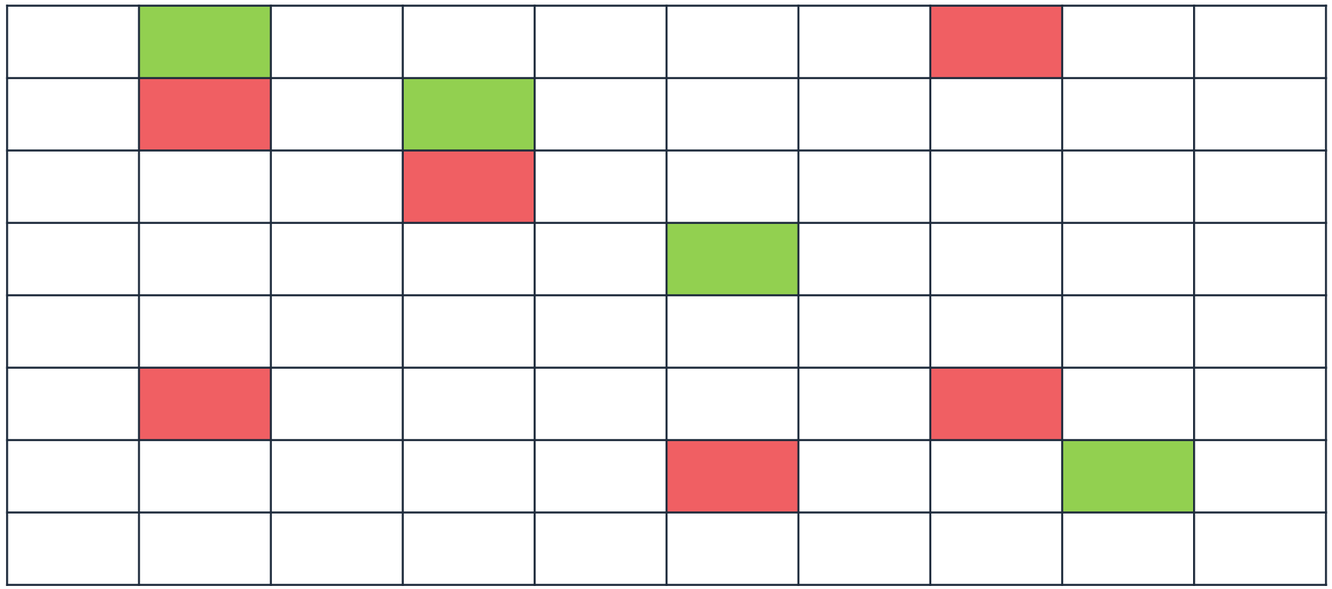
Felles tiltaksbank

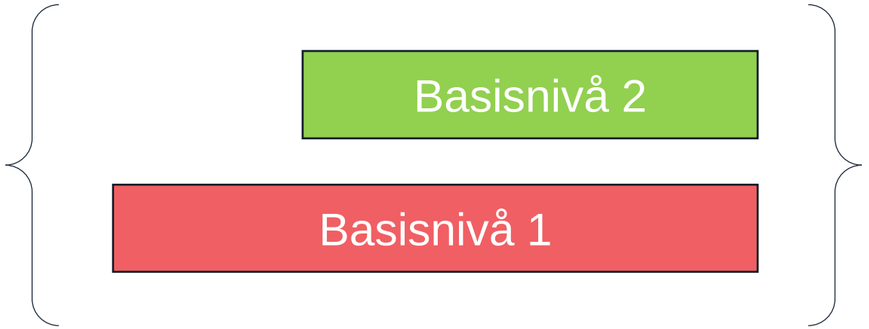


Basisnivå 1

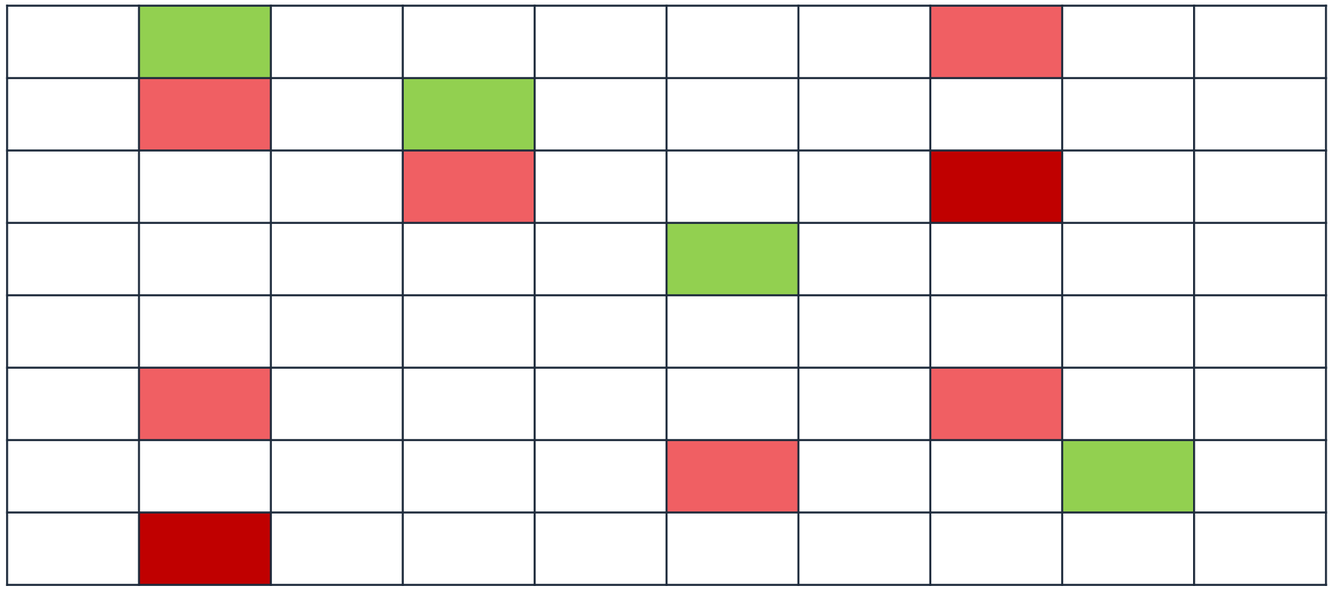


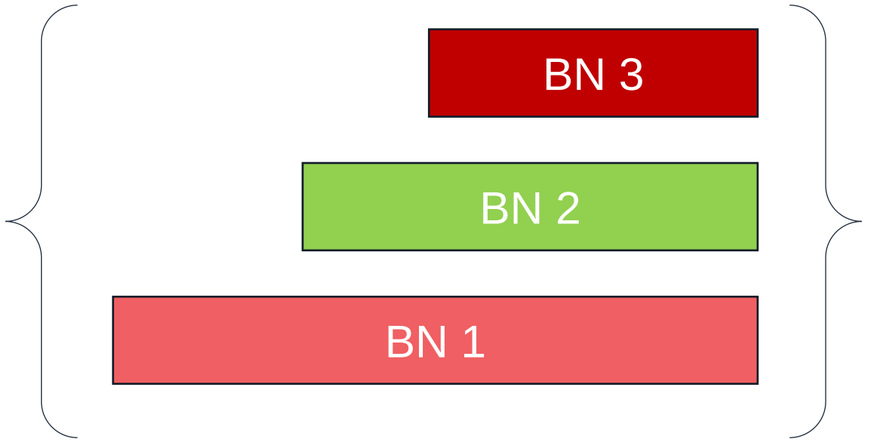
Basisnivå 2



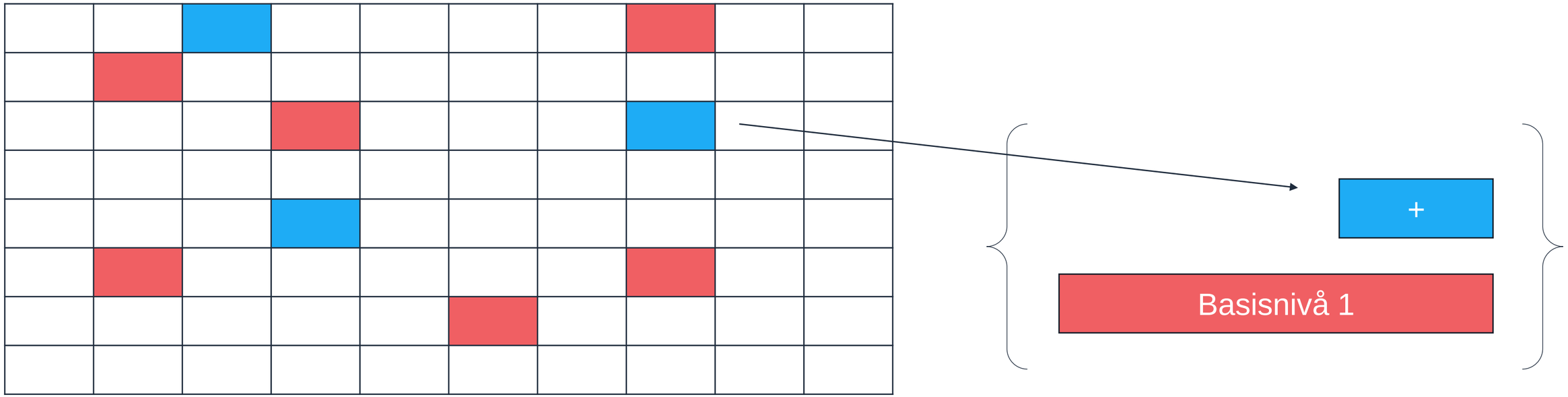


Basisnivå 3





Normen (sikkerhetstiltakene i kap 5)



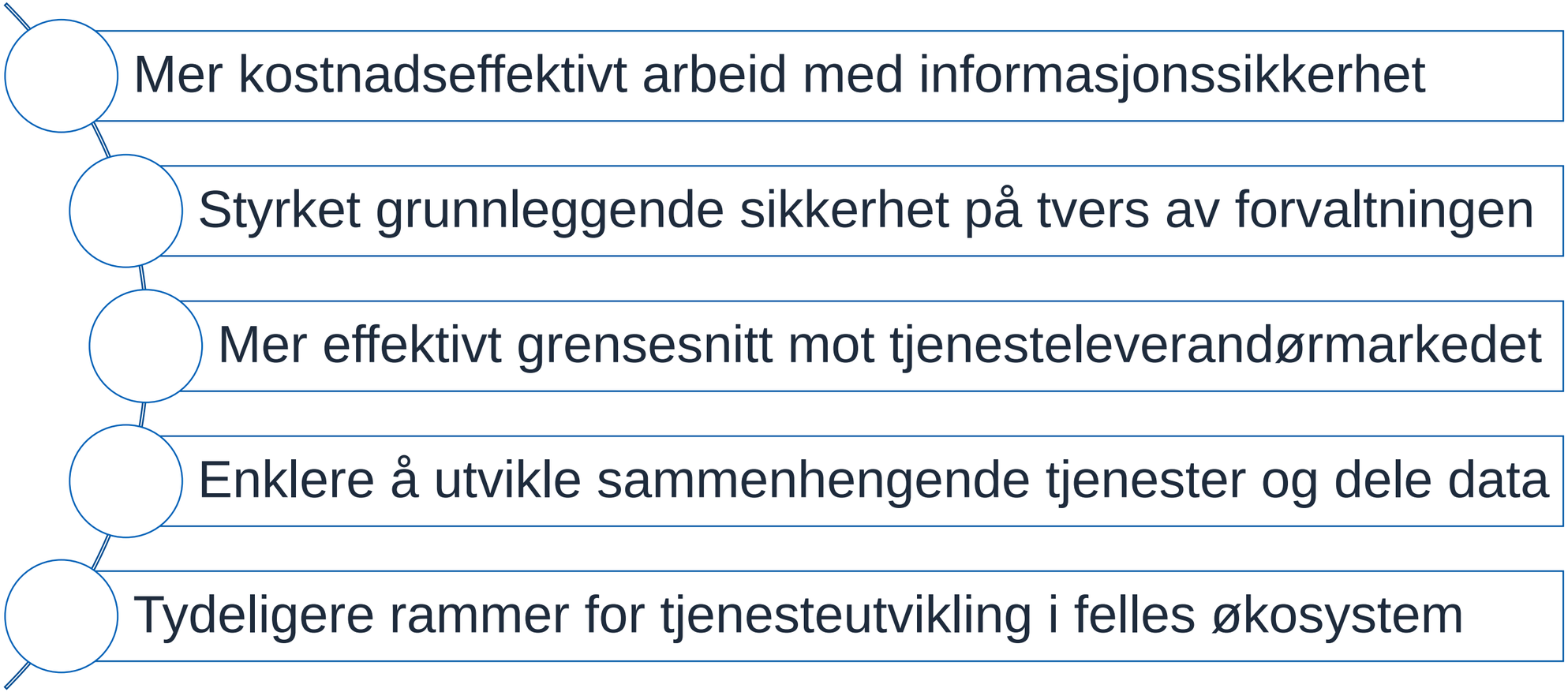
Direktoratet for e-helse kan lage en eller flere spesialtilpassete baselines for helsesektoren. Et slikt basisnivå kan benyttes i stedet for dagens kapittel 5 med krav om spesifikke sikkerhetstiltak.

Digdir

digdir.no

Gevinster

Mulige gevinster



Vurdering av risiko

- Hold oversikt og prioritere
  - Du henter fra katalogen
  - Tilpasser og får oversikt

TORO

posesuppe

Digdir

digdir.no

Hva skjer nå?

Første delprosjekter

Prosjekt

Katalog med oppgaver/tjenester og informasjonstyper

- Digdir, KS/kommuner
- Utforming av prototype/MVP
- Begynne med utvalgte oppgaver og tjenester

Prosjekt

Tydelig felles referanseramme og basisnivåer med sikkerhetstiltak

- Digdir
- Konseptutvikling

Felles sikkerhet i forvaltningen

For spørsmål og innspill:
infosikkerhet@digdir.no

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo