Digdir

digdir.no

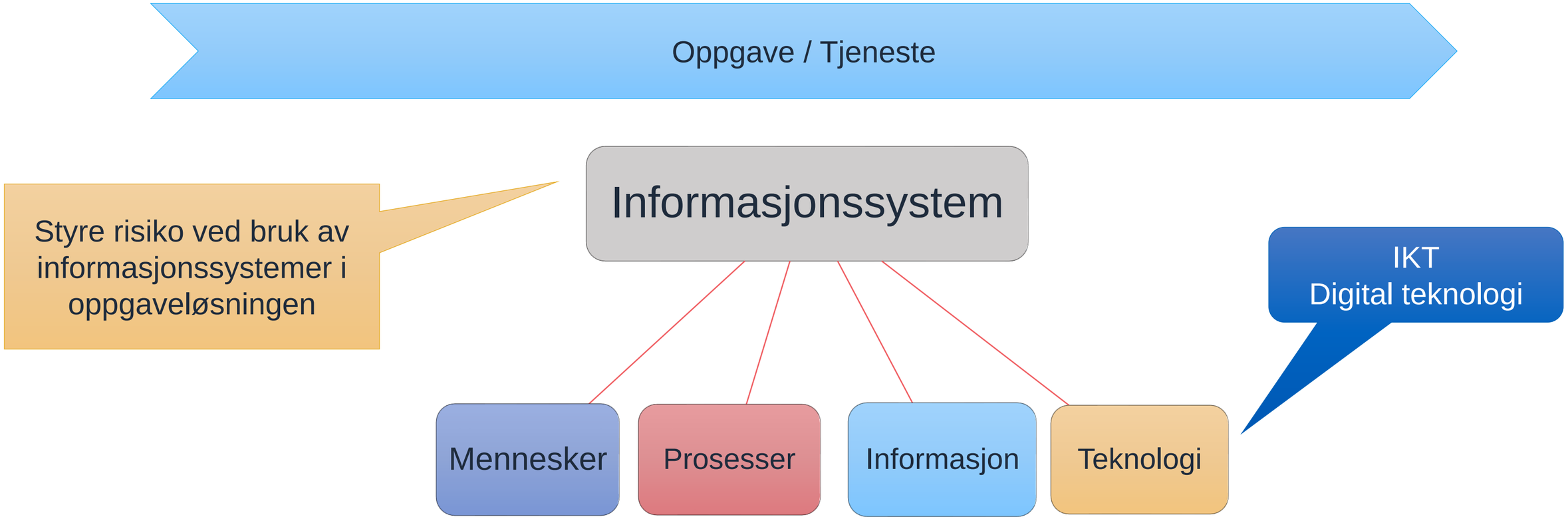
Felles sikkerhet i forvaltningen
-
Katalog over oppgaver og informasjonstyper

Faglig arena for informasjonsforvaltning og deling av data
30.11.2022

Katrine Aam Svendsen, seniorrådgiver

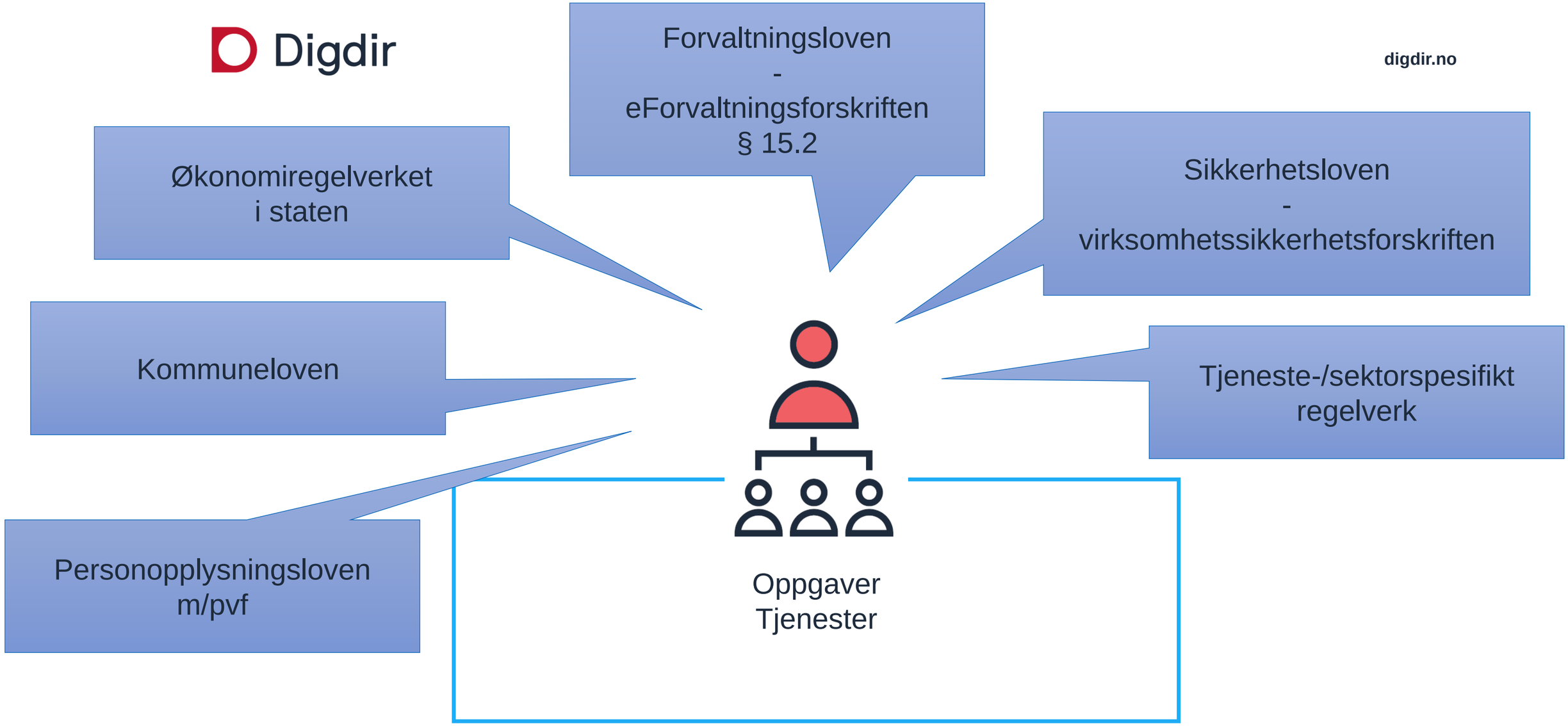
Agenda

- Hvorfor trengs «Felles sikkerhet i forvaltningen»?
- Hvordan kan det gjøres?
  - Katalog over oppgaver og informasjonstyper
- Publisering av notat om Felles sikkerhet i forvaltningen


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

Redskap: risikostyring

Styringsaktiviteter

- Ledelsens styring og oppfølging
- Vurdering av risiko
- Håndtering av risiko
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon

Sikkerhetstiltak

Formål

- Forebygge
- Oppdage
- Håndtere og gjenopprette

Typer

- Organisatoriske
- Menneskelige
- Fysiske
- Teknologiske

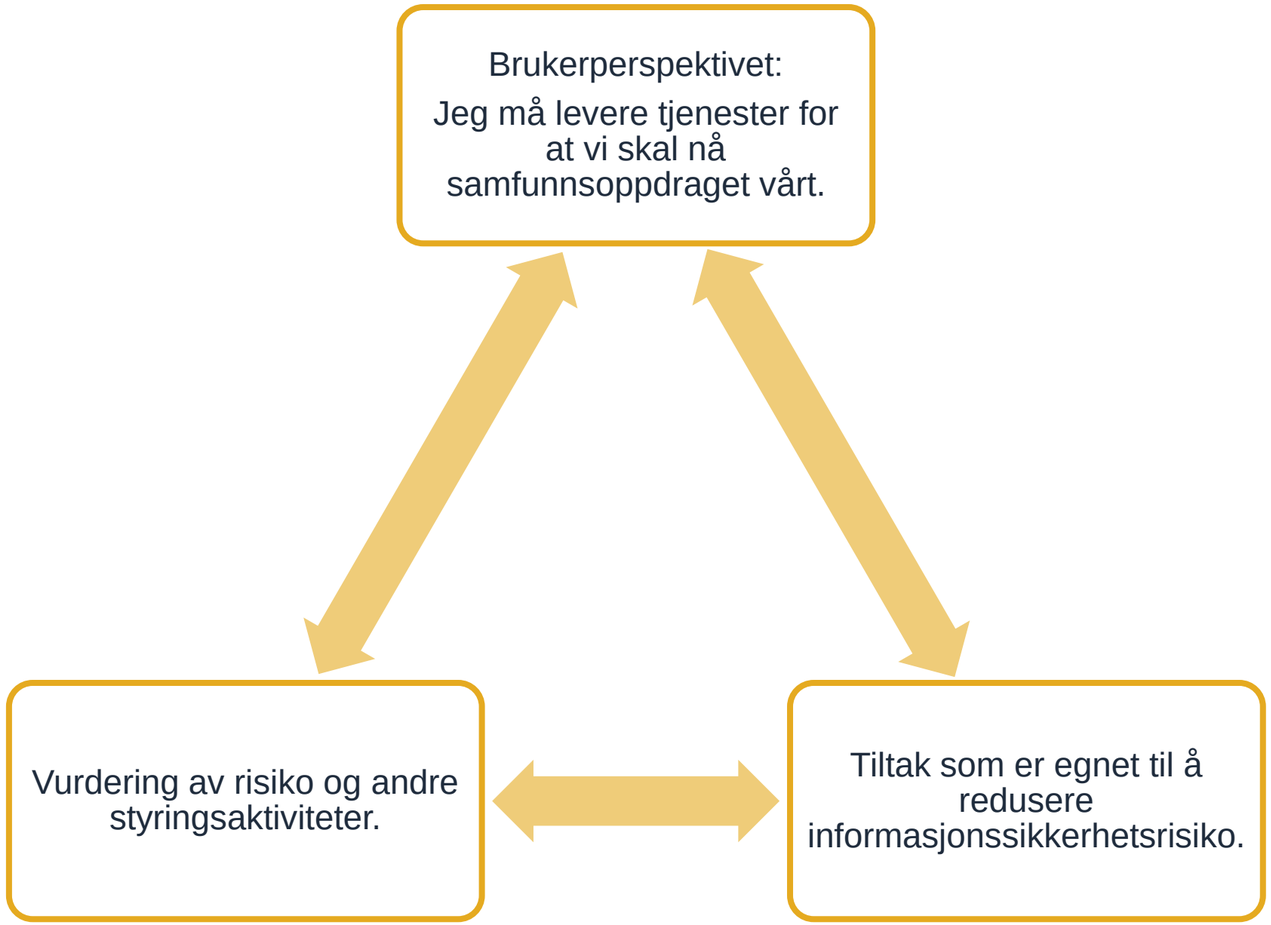
«Erfaring viser imidlertid at anbefalinger og veiledninger i varierende grad blir fulgt opp av virksomheter. Forståelsen for forebyggende digital sikkerhet er begrenset i mange virksomheter, ikke minst på ledelsesnivå.»

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

Felles sikkerhet i forvaltningen

- Et initiativ fra Digitaliseringsdirektoratet
- Konkret veiledning - brukerorientert
- Gjøre like ting likt
- Samarbeid mellom veiledningsaktørene

Virksomhetsperspektivet



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

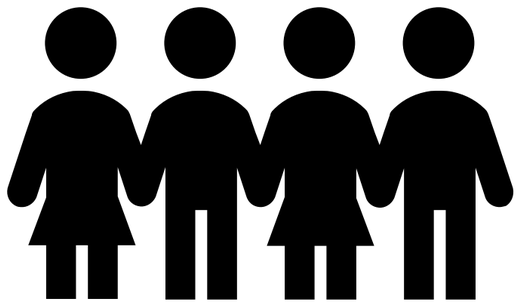
Mangelfull og fragmentert regulering

Tilbakemeldinger fra virksomheter i forvaltningen

Jeg syns dere har en god forståelse av utfordringene kommuner og andre møter.

Dette fokuset har jeg savnet i flere år ☺

Veldig bra at det blir satt søkelys på kompleksiteten og kompetansebehovet i dette arbeidet.



Hvordan kan det gjøres?

Felles sikkerhet i forvaltningen

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.


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

Katalog over oppgaver og informasjonstyper

Katalog

En systematisk oversikt der man kan gjenfinne og gjenbruke informasjonen.

Informasjonstype

grupper av informasjonselementer som inngår i gjennomføringen av en oppgave

Oppgaver

De oppgavene en virksomhet er utfører, eller tjenester de leverer


Ledelsens styring og oppfølging
Vurdering av risiko
Håndtering av risiko
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

Internkontroll – Vurdering av risiko

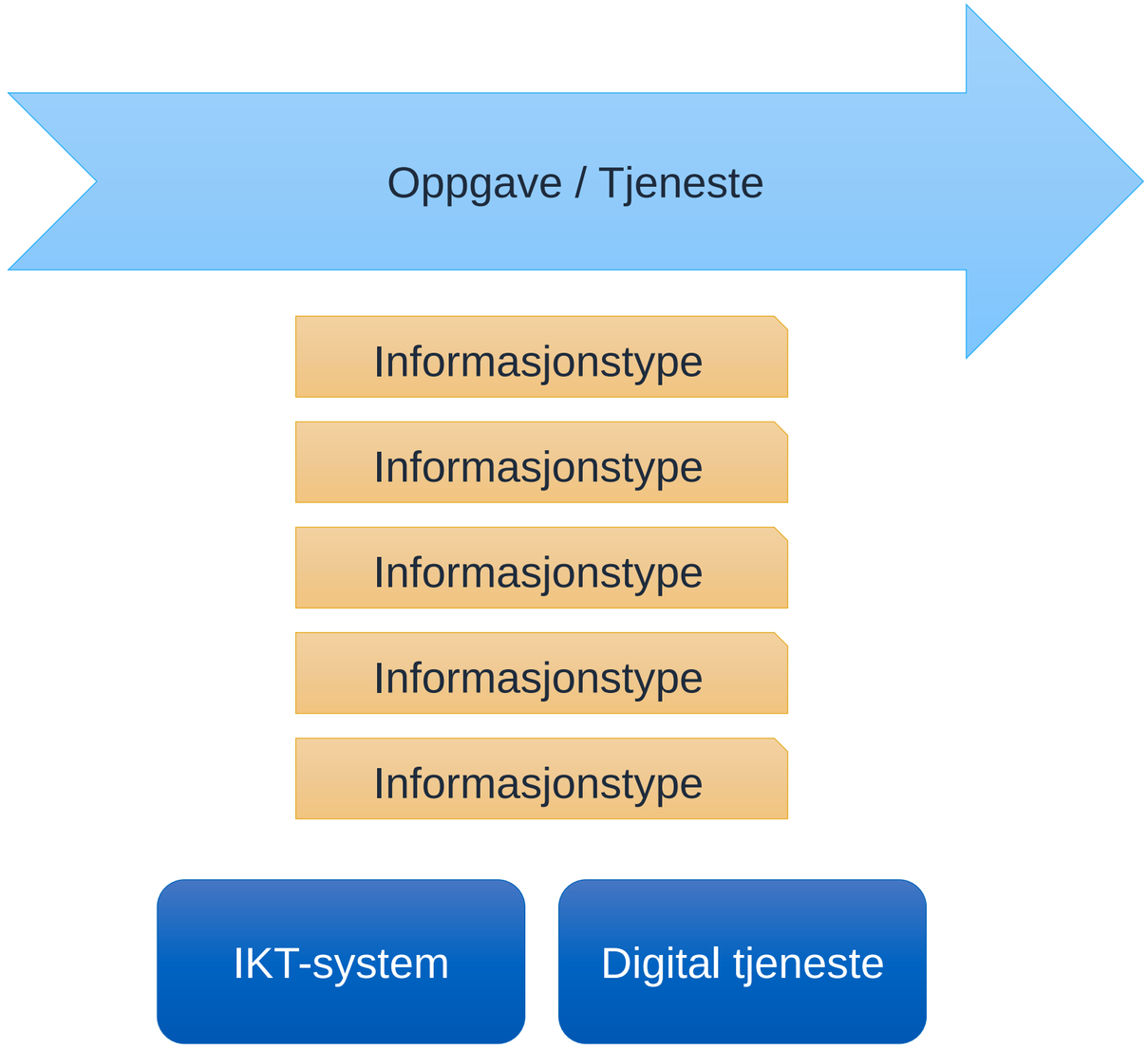
Ha oversikt og prioritere

- Foranalyse av eget ansvarsområde
- Analysere eksterne krav
- Gruppere eller dele opp
- Vurdere behov for risikovurderinger

Planlegge og gjennomføre risikovurderinger

Kan bidra til

- Å redusere omfanget av det som må gjøres i hver enkelt virksomhet
- Å effektivisere arbeidet med informasjonssikkerhet
- Å gi mer like vurderinger og prioriteringer


Oppgave / Tjeneste
Informasjonstype
Informasjonstype
Informasjonstype
Informasjonstype
Informasjonstype
IKT-system
Digital tjeneste

Grunnskole - Elevadministrasjon

- Navn
- Fødselsnummer
- Adresse
- Vurderinger / karakterer
- Vedtak om spesialundervisning

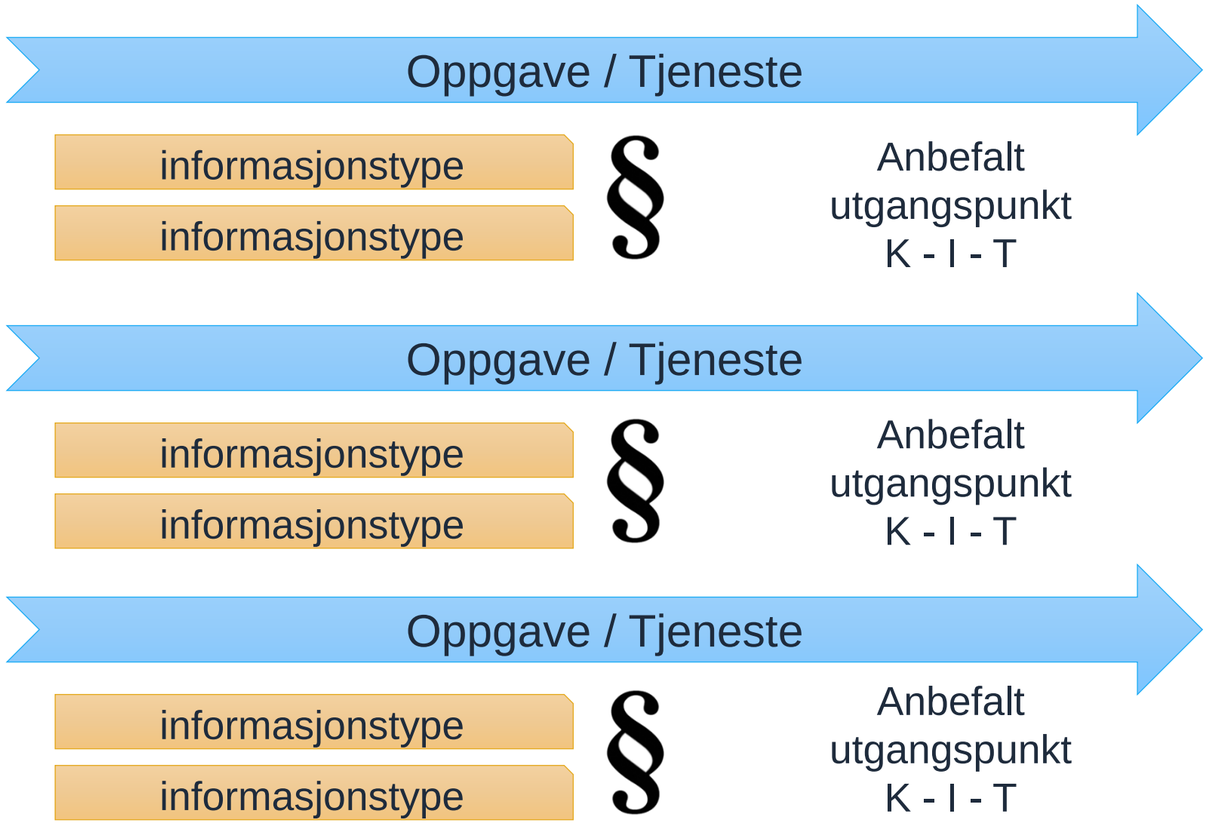
Spesielt obs på K-behov for elever med hemmelig adresse

Spesielt obs på K-behov

IKT-system

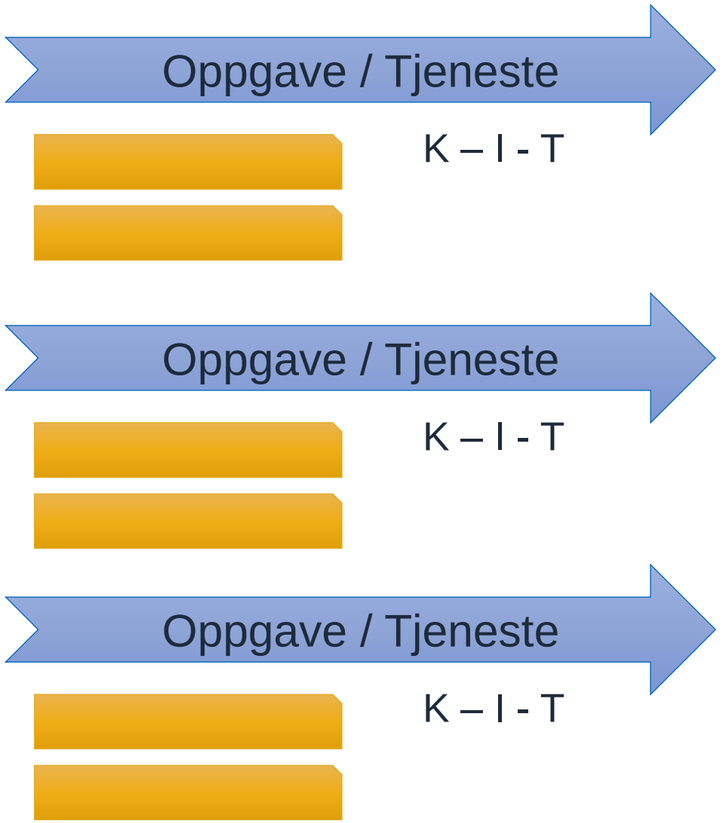
Digital tjeneste

Katalog


Oppgave / Tjeneste
informasjonstype
informasjonstype
§
Anbefalt utgangspunkt K - I - T
Oppgave / Tjeneste
informasjonstype
informasjonstype
§
Anbefalt utgangspunkt K - I - T
Oppgave / Tjeneste
informasjonstype
informasjonstype
§
Anbefalt utgangspunkt K - I - T

Hvilke oppgaver / tjenester?

- Alle offentlige virksomheter har en del av de samme støtteoppgavene
  - Personalforvaltning (HR)
  - Anskaffelser
- Kommuner har ganske like oppgaver / tjenester
- Fylkeskommuner har ganske like oppgaver / tjenester



Virksomhetsstyring

Prosesskartlegging

Oversikt over informasjon som behandles

Prioritering og videre arbeid med informasjonssikkerhet

- Behandlingsprotokoll (personopplysninger)
- Datakatalog/ deling av data
- Arkivering og dokumentasjon
- Sikring etter sikkerhetsloven
- …

Behov for ulikt detaljnivå på ulike områder

Informasjonssikkerhet

Kontaktinformasjon

Deling av data

Fornavn
Etternavn
Gateadresse
Postnummer
Poststed
Telefonnummer

Utkast «prototype»

Beskrivelse av oppgaven/tjenesten	
Navn på oppgaven/tjenesten	Offentlige anskaffelser
Formål	Innkjøp av varer eller tjenester for virksomheten
Kort beskrivelse	Fra identifisering av behov til signert kontrakt

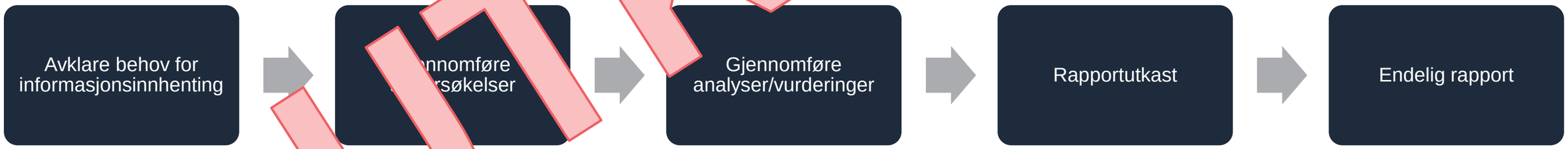
Relevante regelverk	
Regelverk relevant for gjennomføring av oppgaven	Lov og forskrift om offentlige anskaffelser Regelverk om elektronisk faktura i sta Lønns- og arbeidsvilkår ved anskaffels idskraft (g anlegg, renholdskontrakter e.l.)
Krav om taushetsplikt/ unntak fra offentlighet	Offentleglova, forvaltning en (taush døren) Anskaffelsesforskri ten § og 7-4 om tlighet og taushetsplikt – viser til offentleglova og forvaltningsloven
Regelverk med krav til informasjonssikkerhet	Person ingsl verr ordningen (Re knyttet til hetsgra e anskaffelser) el valti forskrifte Krav til kon anseverkt Anskaffelsesforskriften §22

Avklare behov o forberede konkurransen → Konkurranse-gjennomføring → Kontraktsoppfølging

Informasjonstype	Person-opplysninger (J/N)	Særlige kategorier av person-opplysninger (J/N)	Spesielle behov for K-I-T
Forberedelsesdokumentasjon (1)			K – interne dokumenter kan unntas offentlighet etter offentleglova §14 eller §15
Prosessdokumentasjon (2)			
Innspill fra markedsdialog			K – mulige forretningshemmeligheter i markedsdialogen kan være omfattet av taushetsplikt etter forvaltningsloven §13
Konkurransegrunnlag (3)			T – anskaffelsesregelverket stiller krav om tilgang til konkurransegrunnlag, tilleggsinformasjon)
Kommunikasjon om anskaffelsen/konkurransen	Ja		Tilleggsinformasjon til konkurransegrunnlaget skal være tilgjengelig på samme måte som konkurransegrunnlaget – Deler av kommunikasjonen kan være taushetsbelagt etter forvaltningsloven §13, eksempel om man bruker dette til avklaringer av tilbud.
Tilbud under behandling	Ja		K – offentliglova 23 tredje ledd. Kan unnta til anskaffelsen er gjennomført.
Tilbud etter behandling			K – deler kan være unntatt
Evaluering (vurdering og beslutninger) under behandling	Ja		K – Offentleglova 23 tredje ledd
Evaluering (vurdering og beslutninger) etter behandling	Ja		K - Kan være unntatt. Forretningshemmeligheter eller interne vurderinger.
Tildelingsmelding	Ja		T – alle skal får denne samtidig. I - vesentlig at tildelingsmelding ikke blir utsatt for uautoriserte endringer
Kontrakt og signert avtale	Ja		K - Deler kan være unntatt.
Dialog om kontrakten/avtalen	Ja		K – potensielle forretningshemmeligheter i dialogen
Klagebehandling	Ja		K - Deler kan være unntatt offentlighet pga forretningshemmeligheter

Beskrivelse av oppgaven/tjenesten	
Navn på oppgaven/tjenesten	Gjennomføre evaluering
Formål	Dokumentere status på et definert område
Kort beskrivelse	Fra oppdrag/mandat er gitt, til resultatet av evalueringen er levert

Relevante regelverk	
Krav om taushetsplikt/ unntak fra offentlighet	Offentleglova forvaltningsloven
Regelverk relevant for gjennomføring av oppgaven	Utredningsinstruksen
Regelverk med krav til informasjonssikkerhet	eForvaltningsforskriften Pol/pvf

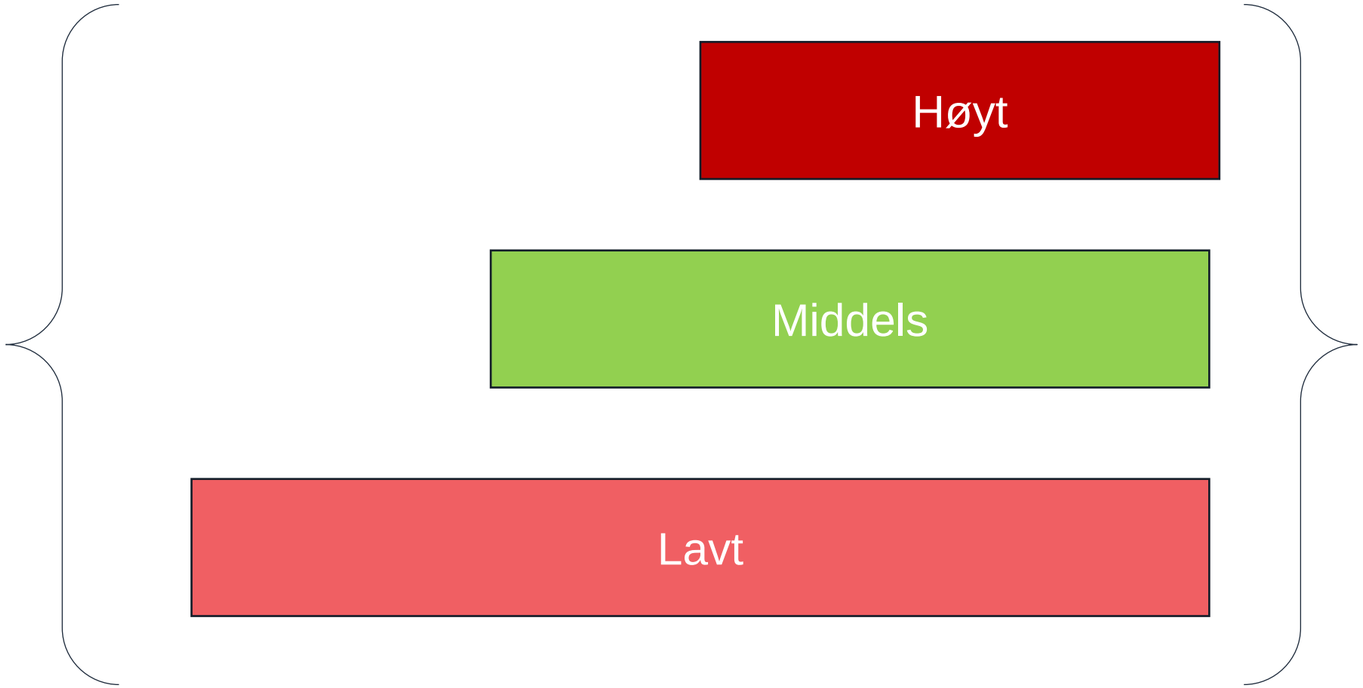


Informasjonsbehandling i oppgaven/tjenesten

Informasjonstype	Personopplysninger (J/N)	Særlige kategorier av personopplysninger (J/N)	Spesielle behov for K-I-T
Mandat	N	N	K – Opp[illegible]n være unntatt offentlighet
Kontaktopplysninger	J	N	
Interne vurderinger/forberedelse (hvilket informasjonsbehov har vi, hva skal vi spørre om etc.)	N	N	K – t[illegible]raget er g[illegible]omført kan interne dokumenter [illegible]tlighet etter offentleglova §14
Dialog med oppdragsgiver	J (kan være kontaktinfo)	N	K – inter[illegible]okumenter kan unntas offentlighet etter [illegible]va §14 eller §15
Spørreskjema, intervjuguide o.l.	N	N	K – interne dokumenter kan unntas offentlighet etter offentleglova §14
Svar fra informanter (svar på spørreundersøkelse, intervjunotater o.l.)	J	N	K – kan være opplysninger underlagt taushetsplikt iht offentleglova §13 jf forvaltningsloven §13
Referat fra intervju	J		K – kan være opplysninger underlagt taushetsplikt iht offentleglova §13 jf forvaltningsloven §13
Anonymisert rådata	N	N	K – interne dokumenter kan unntas offentlighet etter offentleglova §14
Vurderinger og anbefalinger		N	K – interne dokumenter kan unntas offentlighet etter offentleglova §14
Rapportutkast	N	N	K – interne dokumenter kan unntas offentlighet etter offentleglova §14
Endelig rapport	N	N	I – kan være vesentlig at rapport/resultatet ikke blir utsatt for uautoriserte endringer T – avhengig av oppdrag kan tilgjengelighet på resultatet være vesentlig.

Vurdering av konsekvensnivå per oppgave

Konsekvensnivåer



Anbefalte minimumstiltak

Mange tiltaksbanker i bruk i forvaltningen

NIST

SP 800-53 r5

ISO/IEC

27002

NSM
IKT-sikkerhet

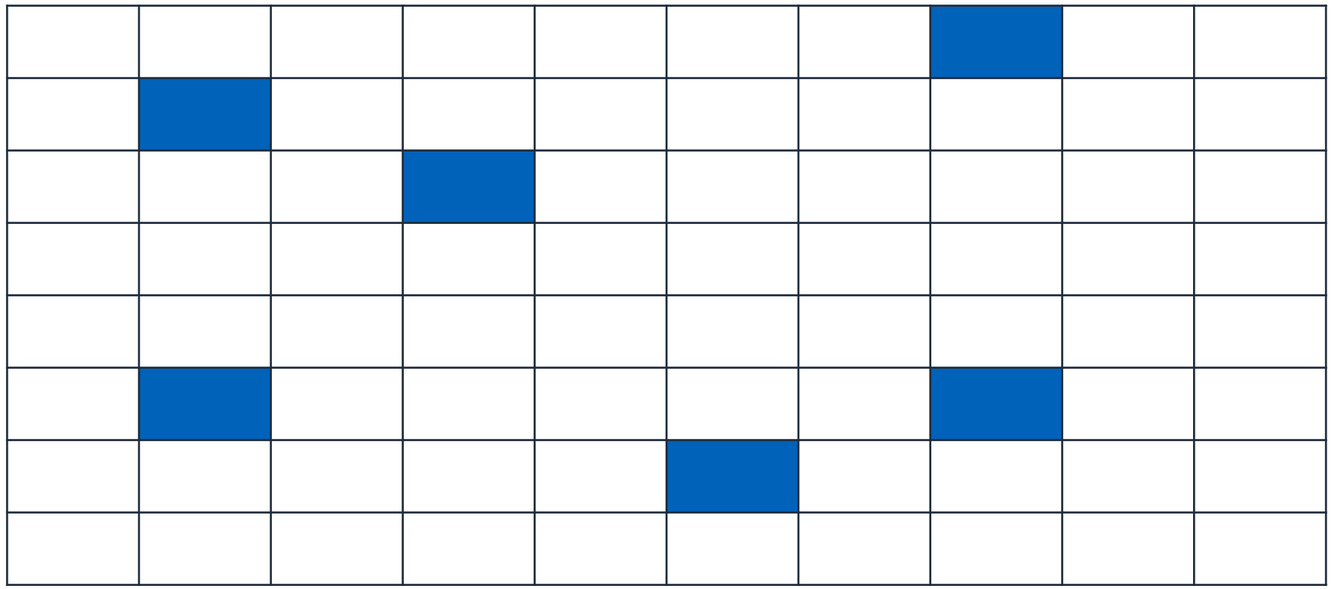
NSM
Fysisk sikkerhet

NSM
Personellsikkerhet

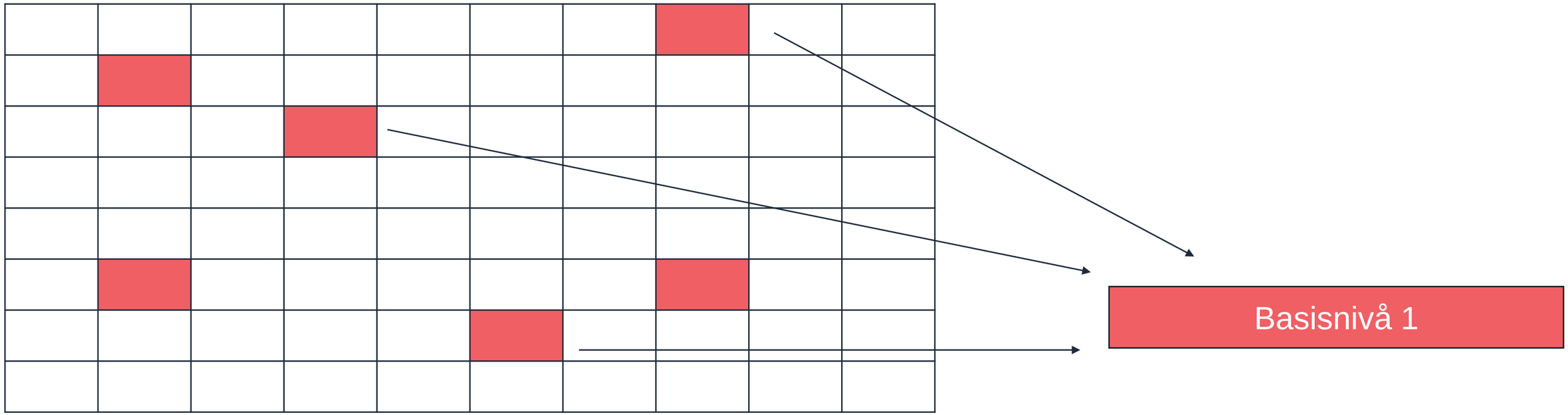
NIST

Cyber Security
Framework

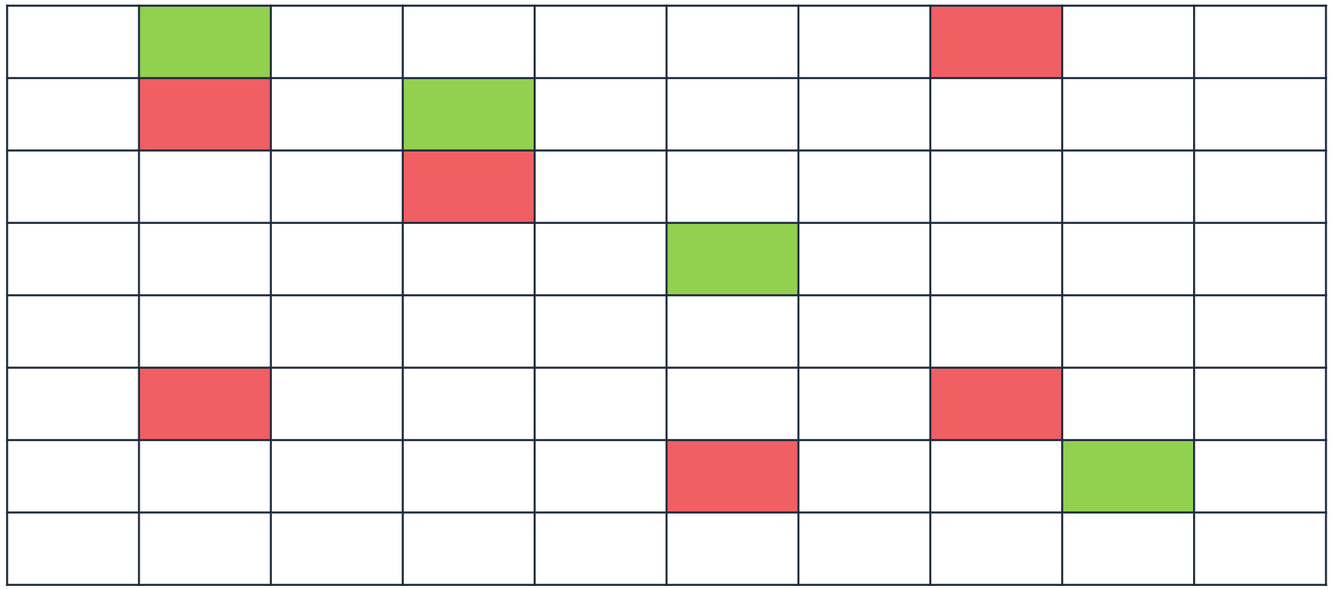
Felles tiltaksbank

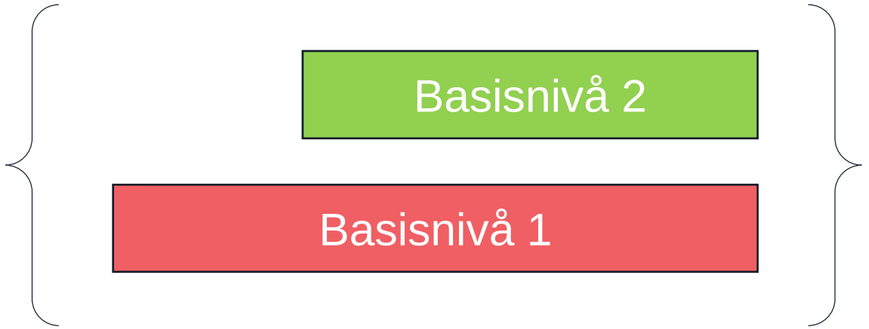


Basisnivå 1

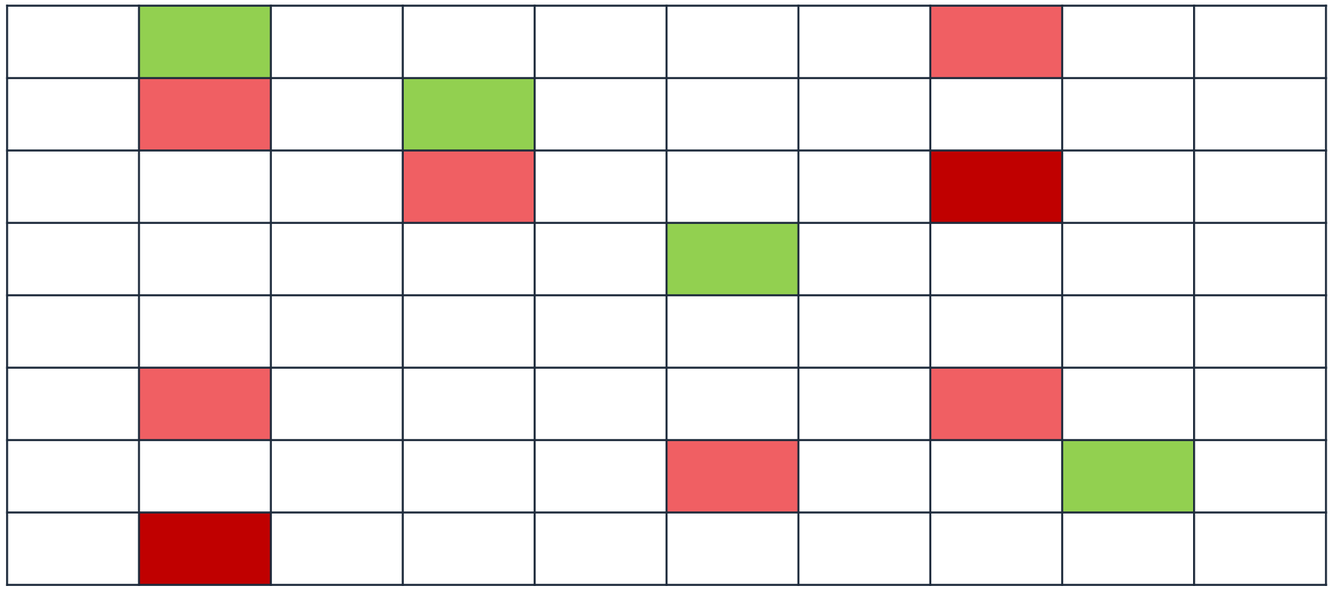


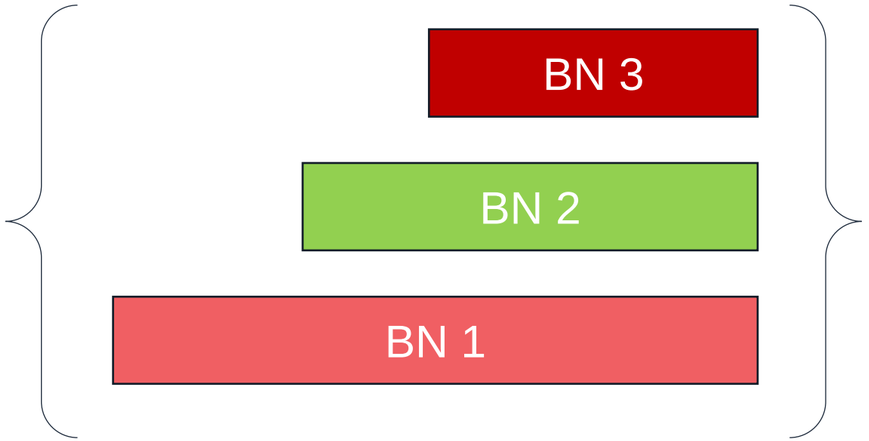
Basisnivå 2





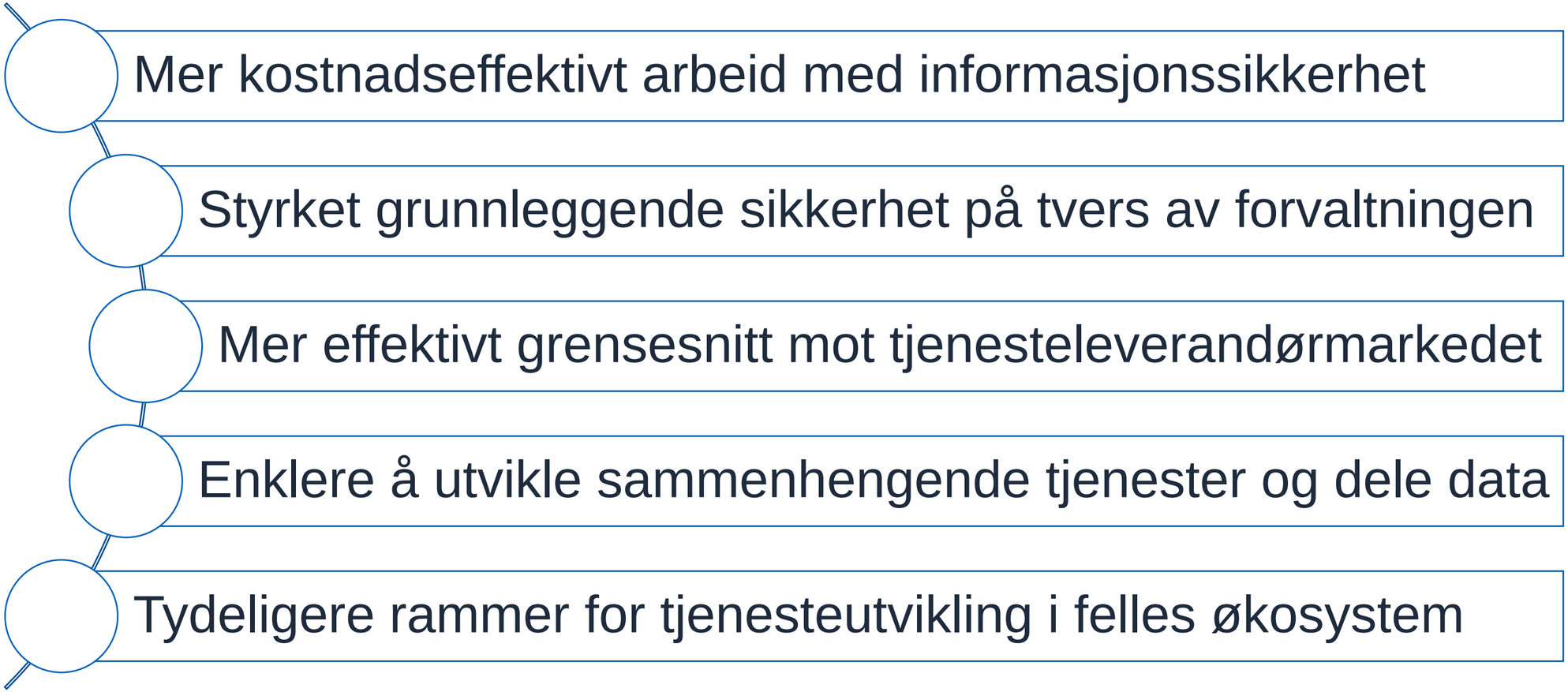
Basisnivå 3





Gevinster

Mulige gevinster



Vurdering av risiko

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

Digdir

digdir.no

Notat – Felles sikkerhet i forvaltningen

Innspillsrunde – sentrale aktører

Datatilsynet er svært positiv til dette arbeidet og ønsker å bidra videre, [..] og [..] å drive de felles prosessene framover.

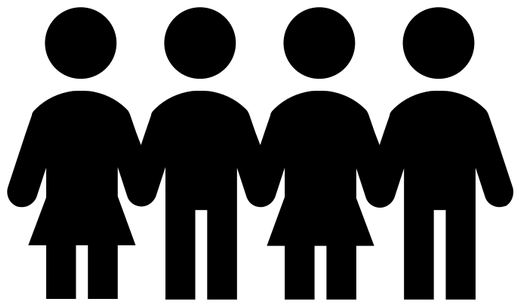
– Datatilsynet

«KiNS stiller seg bak den beskrevne strategiske retningen og mener det et presserende behov for et nasjonalt løft for informasjonssikkerhet generelt og digital sikkerhet spesielt.»

– KiNS

Aktørene må instrueres til å samarbeide og samarbeidet må koordineres.

– Dir for e-helse



KS kjenner igjen utfordringsbildet og støtter direktoratets initiativ for å avhjelpe situasjonen.

– KS

Innspillsrunde – sentrale aktører

«[..] Dette vil gjøre det enklere for virksomhetene å finne riktig nivå for sitt arbeid med informasjonssikkerhet, og også for de forskjellig områdene innenfor informasjonssikkerhet.»

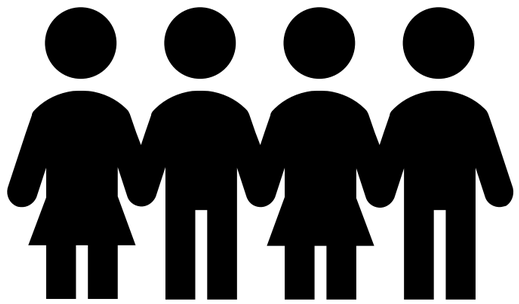
– Datatilsynet

HK-dir deler Digdirs synspunkt om at det er hensiktsmessig for [..] virksomhetene å ha en tydelig, felles referanseramme.

– HK-dir

Vi støtter at Digdir starter arbeidet med å utforme en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter.

– DFØ



Når kommer notatet?

- Første halvdel av desember
- Publiseres på digdir.no

digdir.no/infosikkerhet

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