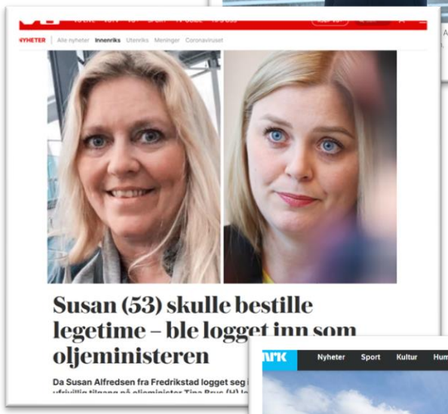
Digdir

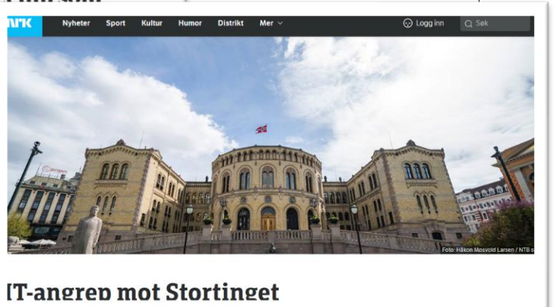
digdir.no

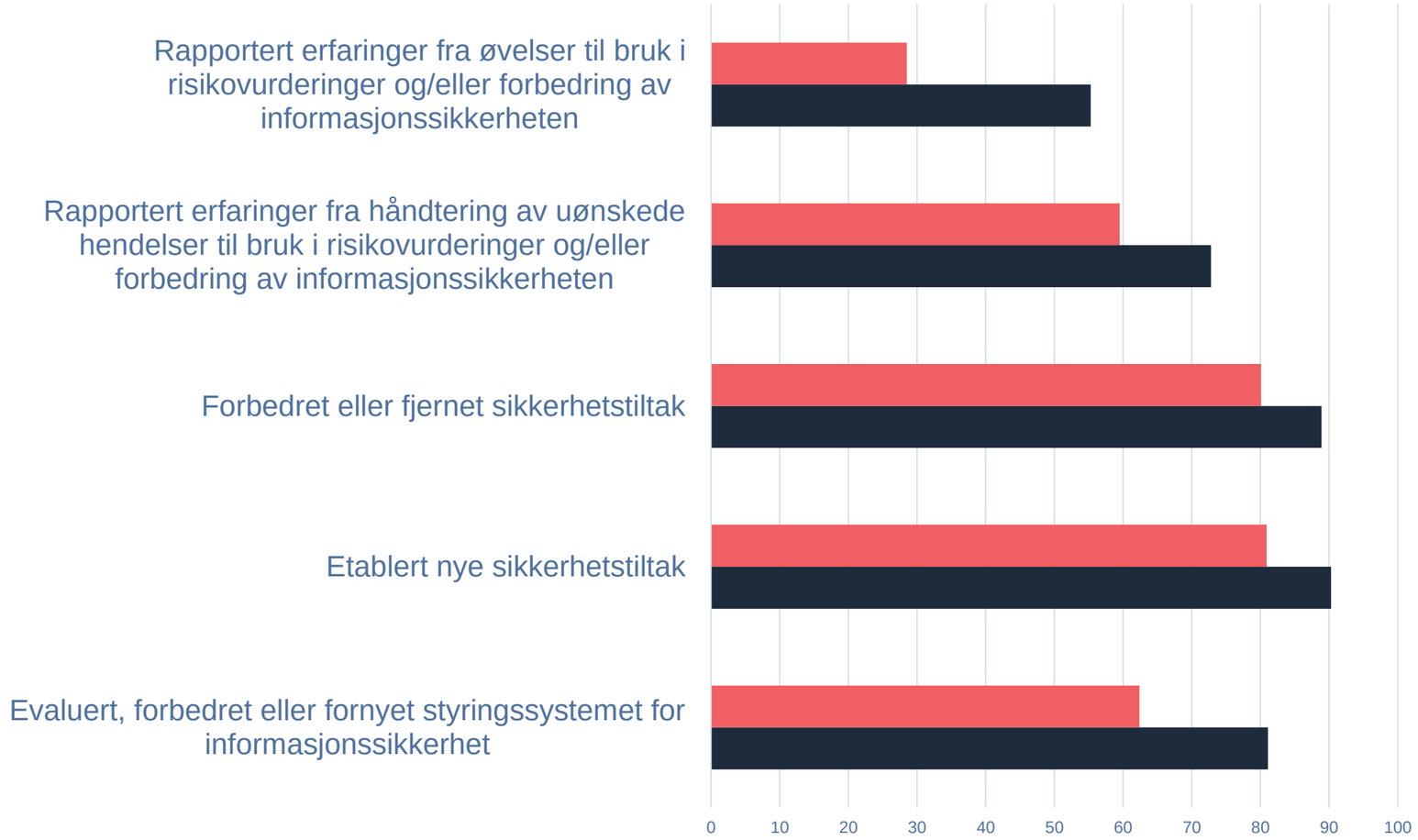
Status og utfordringer i offentlig sektor mht. styring og kontroll på informasjonssikkerhetsområdet – Råd fra Skate

23. mars 2022

Utfordringsbildet







← Til dfo.no

Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen

Skriv ut | Innhold | Søk

1. Om veilederen | 2. Hva og hvorfor er det viktig? | 3. Oppfølging av informasjonssikkerhet | 4. Dialogverktøy | 5. Begrepsforståelse | 6. Krav i regelverk

Om veilederen

Oppdatert 10. feb. 2020

Denne veilederen gir en innføring i informasjonssikkerhet i underliggende virksomheter og viser hvordan departementet kan følge opp informasjonssikkerheten i styringsdialogen. Den kan derfor være nyttig både for deg som er etatsstyrer, og for deg som er ansvarlig for informasjonssikkerheten i en virksomhet.

Innholdsfortegnelse

→ Hvem bør lese denne veilederen?

Hva kan du bruke veilederen til?

Hvem bør lese denne veilederen?

Du bør lese denne miniveilederen hvis du

- er etatsstyrer som skal ivareta departementets overordnede ansvar for oppfølgingen av informasjonssikkerhet i en underliggende etat, for eksempel forberede et etatsstyringsmøte
- lurer på hvordan informasjonssikkerhet bør følges opp, og hvordan temaet bør behandles som en integrert del av virksomhetsstyringen i en underliggende virksomhet
- er leder eller ansvarlig for arbeidet med informasjonssikkerhet i en virksomhet og skal ha dialog med departementet om dette

Hva kan du bruke veilederen til?

Miniveilederen er en hjelp for å
informasjonssikkerhet. Vi har l
tar hensyn til at behovene vari

- Behovet for å følge opp in
departement til departen

ovelse.no

Om ovelse.no | Logg inn | Registrer deg

Velkommen til øvelser for bedre digital sikkerhet

Velkommen til myndighetenes øvingsportal som skal bidra til at alle virksomheter i Norge får et øvingstilbud innen digital sikkerhet. Bruk av øvelser er sentralt element i Nasjonal strategi for digital sikkerhet.

Portalen er laget som et ledd i den nasjonale øvelsen Digital 2020, og her tilbys diskusjonsøvelser basert på ulike scenarier som kan ramme din virksomhet.

Hensikten med øvelsene er at din virksomhet skal få mulighet til å diskutere seg frem til hvordan det er naturlig å håndtere ulike type hendelser. Samtidig får virksomheten din litt støtte på veien i form av diskusjonsspørsmål og råd om hva du bør tenke på for å forberede deg på denne type scenarioer.

Lykke til!

Logg inn | Registrer deg

Hva er en diskusjonsøvelse?

Kom i gang

Forskning og diskusjonsø

enfor info

Digdir

Søk | Meny

Hjem > Informasjonssikkerhet > Kompetanse- og kulturutvikling

Kompetanse- og kulturutvikling innen informasjonssikkerhet

Her finner du veiledning som kan hjelpe deg når du skal arbeide med kompetanse og kultur innen informasjonssikkerhet i din virksomhet.

Kartlegging av digital sikkerhetskultur

Få veiledning om hvordan du kan kartlegge den digitale sikkerhetskulturen i din virksomhet.

Kompetanse- og kulturutvikling innen digital sikkerhet

Få veiledning om hvordan du kan arbeide med utvikling av kompetanse og kultur knyttet til digital sikkerhet.

Virkemidler

Meny

Dialogverktøy – støtte til styringsdialogen om informasjonssikkerhet

Dette dialogverktøyet er et hjelpemiddel til styringsdialogen om informasjonssikkerhet mellom departement og virksomhet. Målgruppen er primært etatsstyrere i departementene, men verktøyet kan også være et nyttig for virksomheter. Dialogverktøyet kan benyttes både som forberedelse til, og i selve styringsdialogen.

Oppdatert 14. des. 2021

Innholdsfortegnelse

→ Dialogverktøyet er delt i to: en hoveddel og en fordypningsdel

Gå videre til de ulike delene

Last ned dialogverktøyet som PDF

Bruk dialogverktøyet sammen med miniveileder

Forarbeid

Hvordan verktøyet kan benyttes

Dialogverktøyet er delt i to: en hoveddel og en fordypningsdel

Dialogverktøyet beskriver hvilke temaer som kan være relevant å ta opp i styringsdialogen. Om temaene skal tas opp, hvordan de skal tas opp og behandles, eller hvilke spørsmål som skal stilles, må – i likhet med all annen etatsstyring – tilpasses egenart, samt risiko og vesentlighet. Verktøyet er ikke uttømmende for alle tenkelige behov, for oppfølgingen av alle statlige virksomheter.

Innholdet er basert på krav og anbefalinger i lov, forskrift og veiledninger. Det er likevel ikke ment å fungere som en fasit, men som et hjelpemiddel til dialog mellom departement og underliggende virksomhet.

Alt i dialogverktøyet handler om arbeidet med informasjonssikkerhet i en virksomhet. For eksempel, der «styring og kontroll» er brukt, så menes det «styring og kontroll på informasjonssikkerhetsområdet».

Gå videre til de ulike delene

Hoveddel – styringsdialog om informasjonssikkerhet →

Fordypning i temaer knyttet til informasjonssikkerhet →

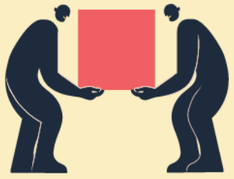
Digdir

Søk | Meny

Hjem > Informasjonssikkerhet > Styring av informasjonssikkerhet > Helhetlig styring og kontroll

Helhetlig styring og kontroll av informasjonssikkerhet

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



Hva vil det si?

Å jobbe helhetlig betyr at man skal se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

Hva er felles?

De samme grunnreglene gjelder uavhengig av hvilket fagområde man skal drive styring og kontroll på. Les mer om fellestrekkene her.

Hva er ulikt?

Helheten er ikke den samme for alle, og ulike perspektiver gir ulikt fokus. Les mer om noe av det som må tas hensyn til dersom man skal lykkes med å jobbe helhetlig.

Hvor får du hjelp?

Aktører som veileder innen styring og kontroll

DFØ, Digitaliseringsdirektoratet, KS, NSM og Datatilsynet har alle veiledning som er relevant når man jobber med ulike deler av informasjonssikkerhet.

→

Om denne veiledningen

Denne veiledningen er resultatet av et samarbeid mellom NSM, DFØ og Digitaliseringsdirektoratet. Datatilsynet og KS har også bidratt i arbeidet.

→

Kompetansebeskrivelser

- Rolle: Fagansvarlig informasjonssikkerhet
- Rolle: Rådgiver informasjonssikkerhet
- Rolle: Risikoeier
- Rolle: Topplеder
- Rolle: Øvrig ledergruppe
- Rolle: IT-leder
- Rolle: Systemeier
- Rolle: Alle ansatte

Rolle: Fagansvarlig informasjonssikkerhet

Fagansvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

Ansvar og oppgaver

Hvilken stilling den fagansvarlige har i virksomheten, vil variere avhengig av virksomhetens organisering og behov. Dersom fagansvarlig har en stilling som leder i virksomheten, vil oppgavene og ansvaret komme i tillegg til oppgaver og ansvar vedkommende har som følger stillingsbeskrivelsen.

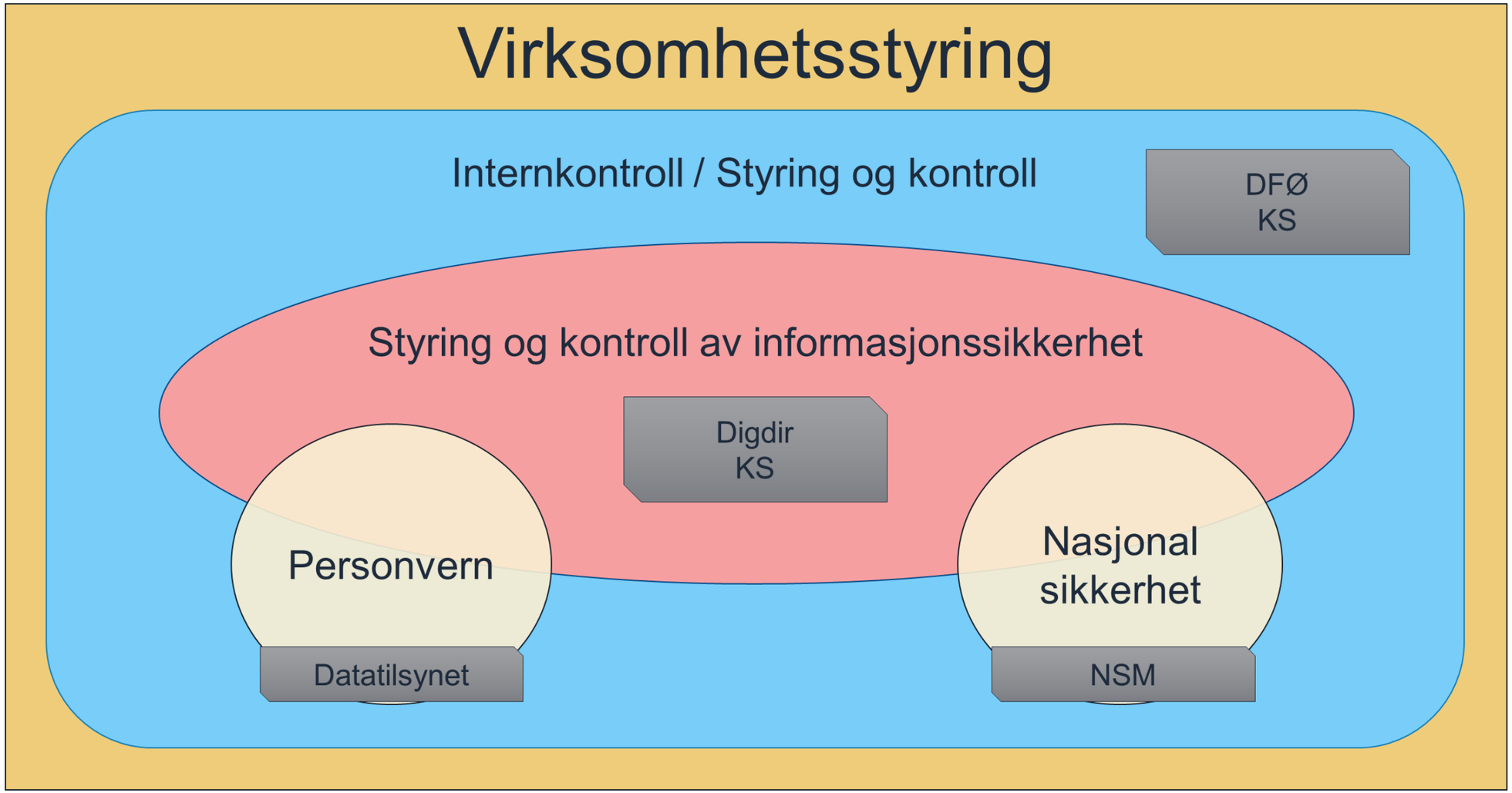
Fagansvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging.

I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon. Fagansvarlig har ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.

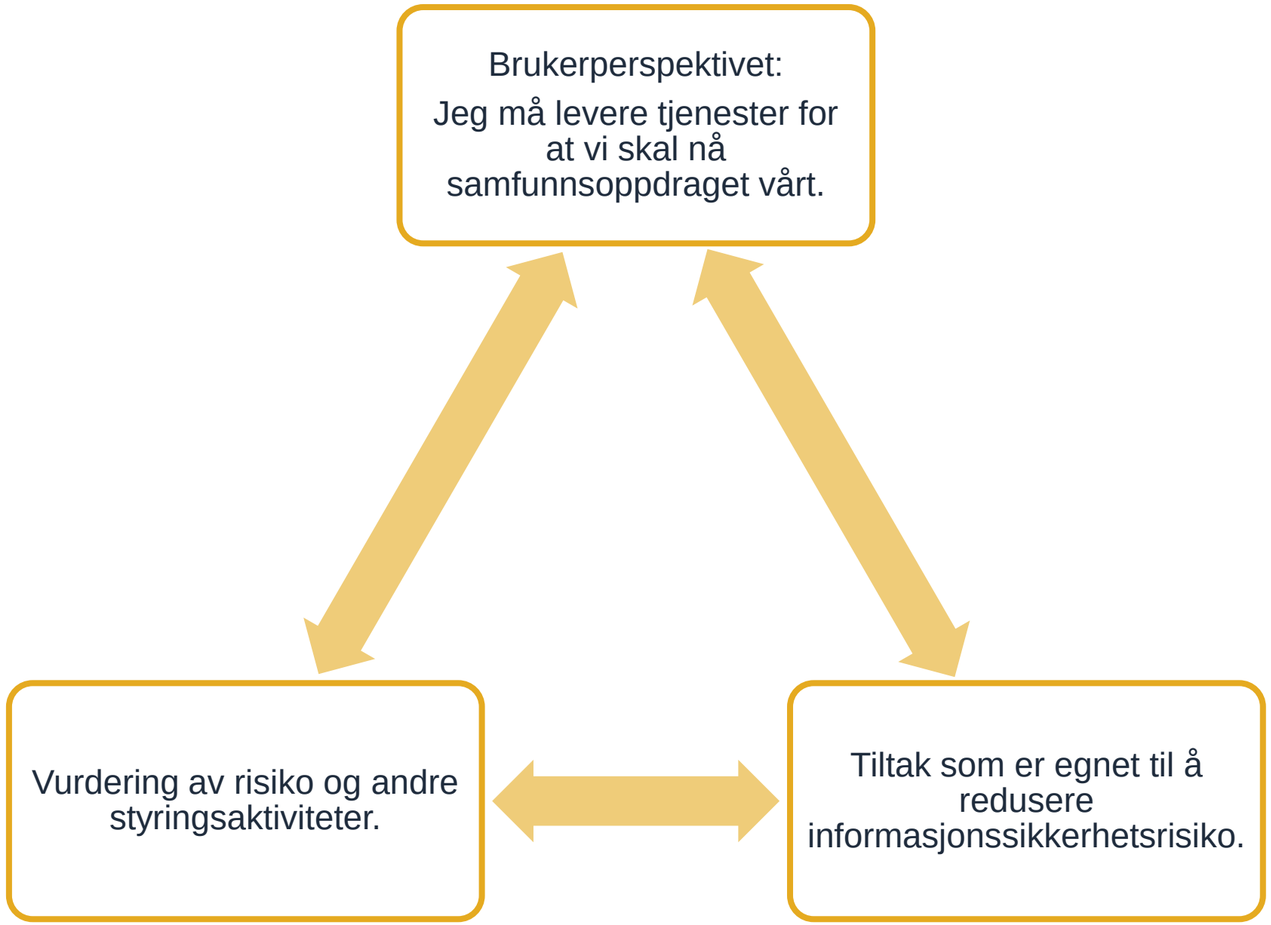
Ønsket kompetanse

Fagansvarlig informasjonssikkerhet er ikke en IKT-teknisk rolle. Den krever imidlertid god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. I tillegg må fagansvarlig informasjonssikkerhet ha god forståelse for

Aktørkart


Virksomhetsstyring
Internkontroll / Styring og kontroll
DFØ
KS
Styring og kontroll av informasjonssikkerhet
Digdir
KS
Personvern
Datatilsynet
Nasjonal
sikkerhet
NSM

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 informasjons-sikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?

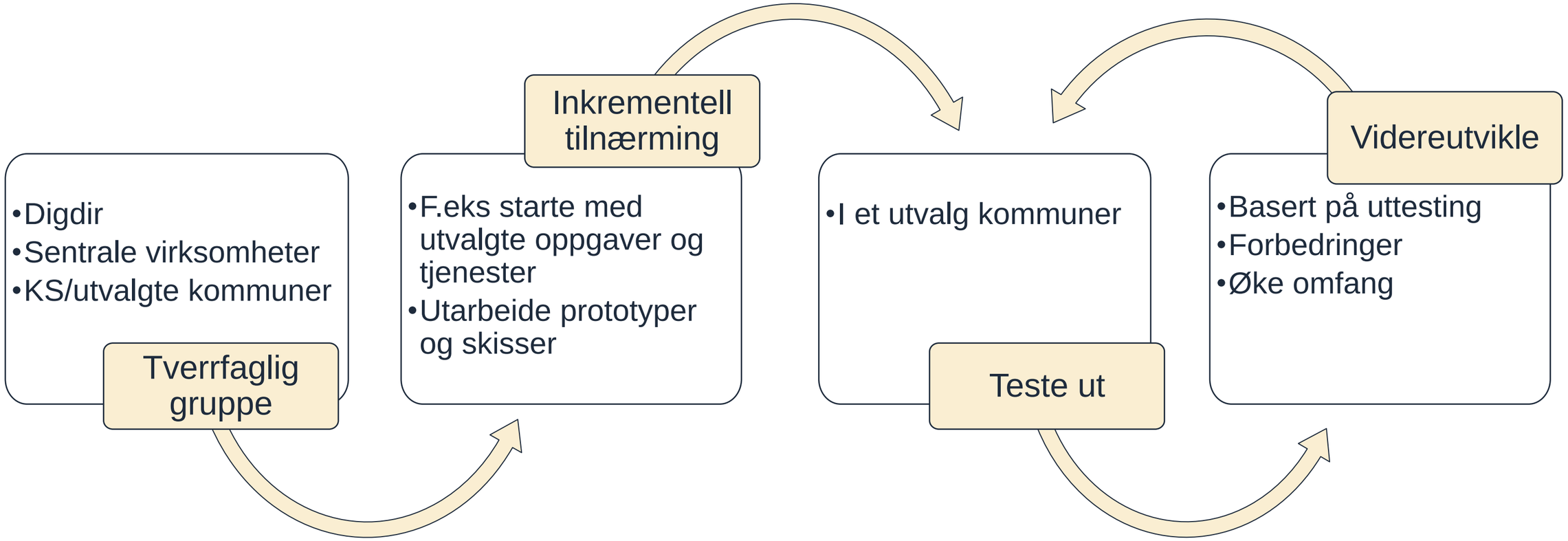
Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave

Anbefalte minimumstiltak

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

Iterativt arbeid med brukerinvolvering



Mulige gevinster

- Mer konkret og enklere å forholde seg til for små og mellomstore virksomheter
- Mer kostnadseffektivt arbeid med informasjonssikkerhet
- Styrket grunnleggende sikkerhet på tvers av forvaltningen
- Mer effektivt grensesnitt mot tjenesteleverandørmarkedet
- Enklere å utvikle sammenhengende tjenester og dele data
- Tydeligere rammer for tjenesteutvikling i felles økosystem

Digdir ønsker følgende råd fra Skate

- Stiller Skate seg bak forslaget til strategisk retning?
- Hvilke justeringer bør Digdir eventuelt gjøre for å treffe offentlige virksomheters behov best mulig?

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