Digdir

digdir.no

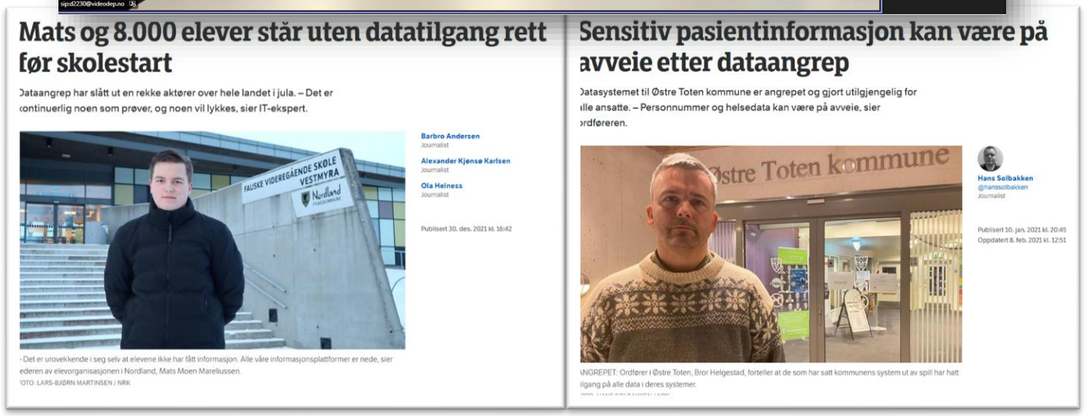
«Katalog over oppgaver og informasjonstyper»

Informasjonssikkerhet

NIFS-møte
14.09.2022

Bakgrunn

Informasjonssikkerhet satt på agendaen



Mats og 8.000 elever står uten datatilgang rett før skolestart

Dataangrep har slått ut en rekke aktører over hele landet i jula. – Det er kontinuerlig noen som prøver, og noen vil lykkes, sier IT-ekspert.

Barbro Andersen
Journalist
Alexander Kjønsø Karlsen
Journalist
Ola Heiness
Journalist

Publisert 30. des. 2021 kl. 16:42

FALSKE VIDEREGÅENDE SKOLE VESTMYRA
Nordland

- Det er urovekkende i seg selv at elevene ikke har fått informasjon. Alle våre informasjonsplattformer er nede, sier ederen av elevorganisasjonen i Nordland, Mats Moen Mørkliussen.

FOTO: LARS-BJØRN MARTINSEN / NRK

Sensitiv pasientinformasjon kan være på avveie etter dataangrep

Datasystemet til Østre Toten kommune er angrepet og gjort utilgjengelig for alle ansatte. – Personnummer og helsedata kan være på avveie, sier ordføreren.

Østre Toten kommune

Hans Solbakken
@hanssolbakken
Journalist

Publisert 10. jan. 2021 kl. 20:45
Oppdatert 8. feb. 2021 kl. 12:51

INGREPET: Ordfører i Østre Toten, Bror Helgestad, forteller at de som har satt kommunens system ut av spill har hatt igang på alle data i deres systemer.

- Tidlig 2022; JD og KDD holdt et møte om digital sikkerhet i kommunene. 200 rådmenn og ordførere deltok digitalt. De fikk høre innlegg fra Østre Toten kommune, KS, NSM og Digdir.
- Bjørn Arild Gram nevnte blant annet Felles Sikkerhet i Forvaltningen (FSiF) som et tiltak for å samkjøre og konkretisere veiledningen overfor kommunene.
- Orienteringsmøte med kommuner og statlige virksomheter om Felles Sikkerhet i Forvaltningen (FSiF). Ca 140 deltakere i møtet, fra over 100 påmeldte virksomheter.

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.

Eksisterende veiledning

1.1.6 Kartlegg informasjonsbehandling og dataflyt i virksomheten. Kartlegg informasjonsflyt mellom arbeidsprosesser, brukere, enheter og tjenester og bruk resultatet som grunnlag for etablering av en sikker IKT-arkitektur, se prinsipp 2.2 - Etabler en sikker IKT-arkitektur.

NSM - Grunnprinsipper for IKT-sikkerhet; 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer

Anbefalte tiltak:

- Identifiser virksomhetens viktigste funksjoner
- Identifiser hvilke verdier som understøtter disse funksjonene
- Vurder konsekvens ved bortfall av verdiene
- Ranger verdiene for prioritering av tiltak

NSM - Grunnprinsipper for sikkerhetsstyring; 1.2 Identifisere verdiene

A: Skaffe oversikt over

- sentrale lover og regler – og ha kunnskap om hvilken betydning de har for kommunen.
- sentrale informasjonsverdier og vurdere deres kritikalitet for kommunens drift og tjenesteproduksjon. Herunder etablere en oversikt over behandling av personopplysninger i kommunen.

KS – Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Etabler felles forståelse for aktuell arbeidsprosess

De som deltar i risikovurderingen bør ha en ensartet og felles forståelse for hvordan vedkommende prosess faktisk gjennomføres og fungerer. Start derfor gjerne med en gjennomgang av den aktuelle prosessen eller aktiviteten.

KS – Orden i eget hus; Kommunedirektørens internkontroll. Kapittel 7.1 Kartlegge risiko

Control

An inventory of information and other associated assets, including owners, should be developed and maintained.

Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

ISO 27002; Kontroll 5.9 Inventory of information and other associated assets

Når man skal kartlegge prosessen, er det viktig å beskrive følgende:

- målet med prosessen
- hvem som er ansvarlig for prosessen (helheten)
- hvor prosessen starter (input) og hvor den slutter (output)
- hvilket detaljnivå den skal beskrives på
- aktivitetene i prosessen
- hvem som er involvert i de ulike aktivitetene
- hvilke system/verktøy som benyttes

DFØ – Prosesskartlegging – Steg 1 – Kartlegge prosessen

I slike tilfeller vil prosesseiere og/eller ledere på lavere nivåer vanligvis få i oppgave å følge opp ledelsens føringer gjennom å vurdere nærmere hvorvidt etablert internkontroll *i* og *i tilknytning til* de utvalgte prosessene er tilfredsstillende.

Som grunnlag for en risikovurdering av operative prosesser er det nyttig å ha en oversikt over:

- mål for prosessen
- hvilke aktiviteter som inngår i prosessen
- hvilke risikoer prosessen er eksponert for
- hvilke kontroller og øvrige risikoreduserende tiltak som eksisterer

Dersom det ikke foreligger noen slik oversikt, kan det være hensiktsmessig å gjennomføre en prosesskartlegging hvor disse elementene identifiseres og dokumenteres.

DFØ - Hvordan utføre internkontroll? 4.2.2 Gjennomføre risikovurderinger

Arkivverket – Metode for identifisering og sikring av dokumentasjon

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

Foranalyse av eget ansvarsområde

1 Identifiser oppgaver og informasjonstyper

Identifiser hvilke oppgaver og tjenester som utføres.

Identifiser hvilke informasjonstyper som behandles i de ulike oppgavene.

2 Finn høyeste konsekvensnivå

Finn høyeste konsekvensnivå brudd på konfidensialitet, integritet og tilgjengelighet kan medføre.

3 Vurder trusler, farer og sårbarheter

Vurder motivasjon, vilje og kapasitet til ulike trusselaktører.

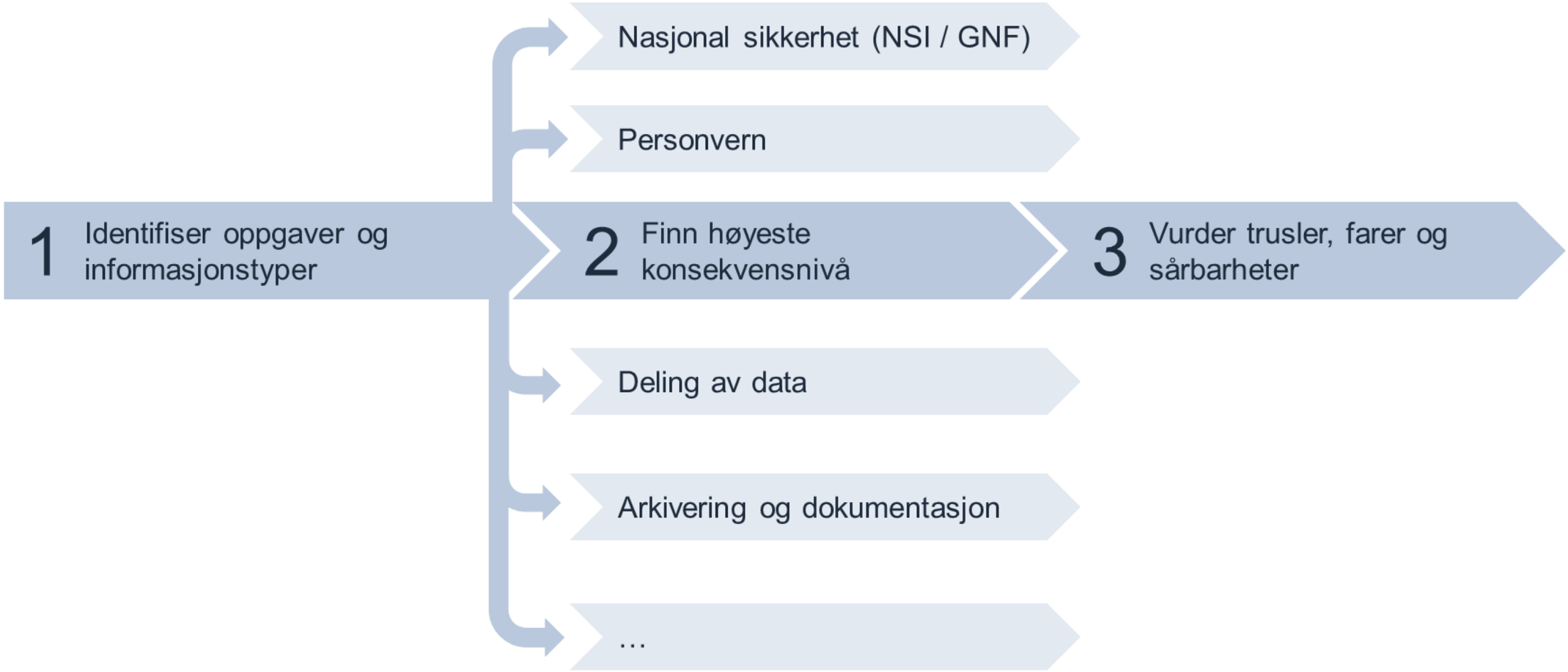
Vurder sannsynligheten og forventet skadenivå for at en spesifikk fare skal inntreffe.

Vurder sårbarhetsnivået basert på oppnåelse av overordnede målsetninger for sikkerhetsarbeidet

Målsetning – ha oversikt for å kunne prioritere riktig!

https://www.digdir.no/informasjonssikkerhet/foranalyse-av-eget-ansvarsomrade/2642
https://www.digdir.no/informasjonssikkerhet/malar-og-eksempel/3164#vurdering_av_risiko

Prioritere videre arbeid – på ulike områder



https://www.digdir.no/informasjonssikkerhet/trinn-1-identifisere-oppgaver-og-informasjonstyper/2643#hvordan_bruke_trinn_1_som_utgangspunkt_for_arbeid_paa_andre_omraader

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

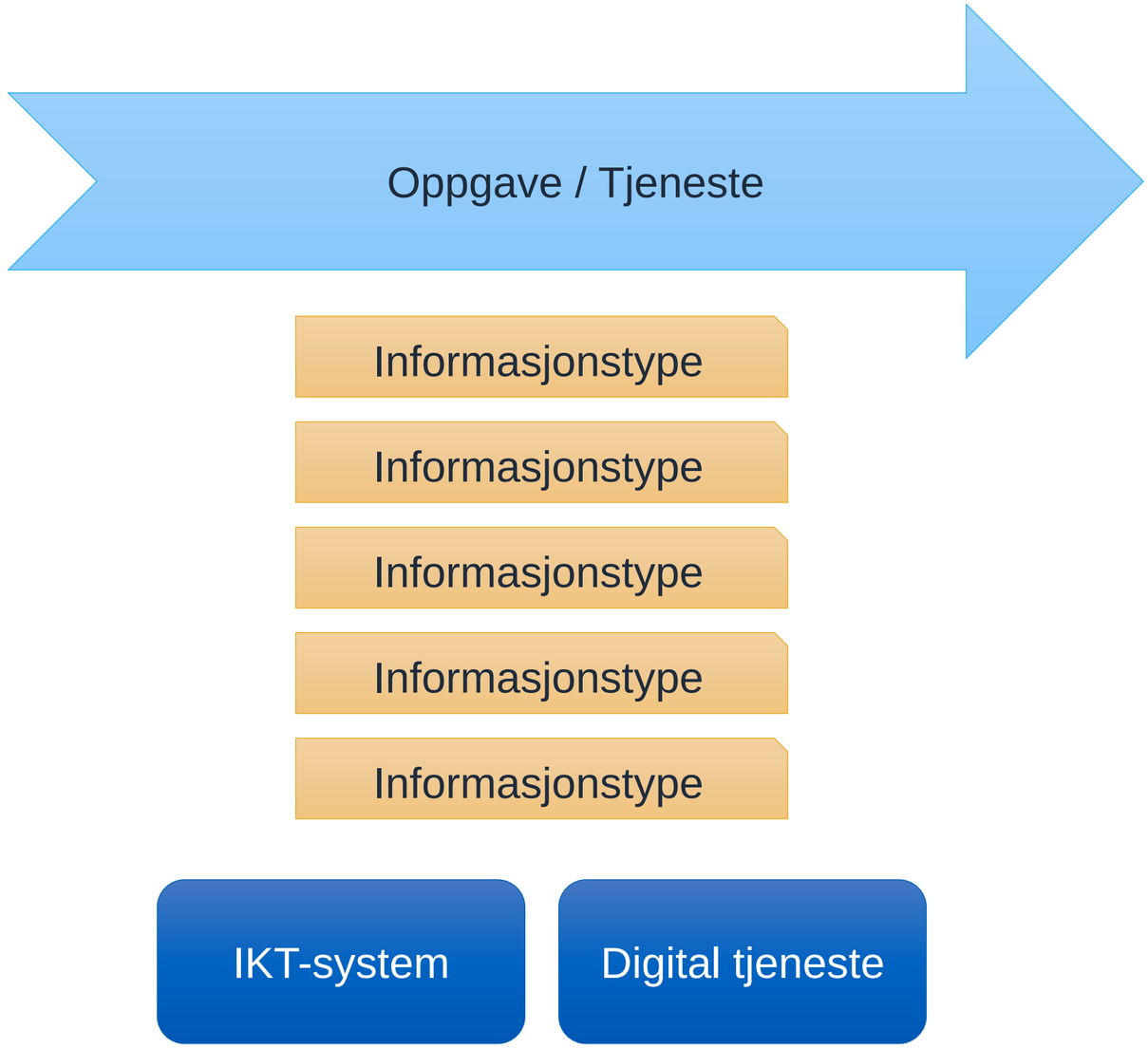
Katalogen – form og innhold

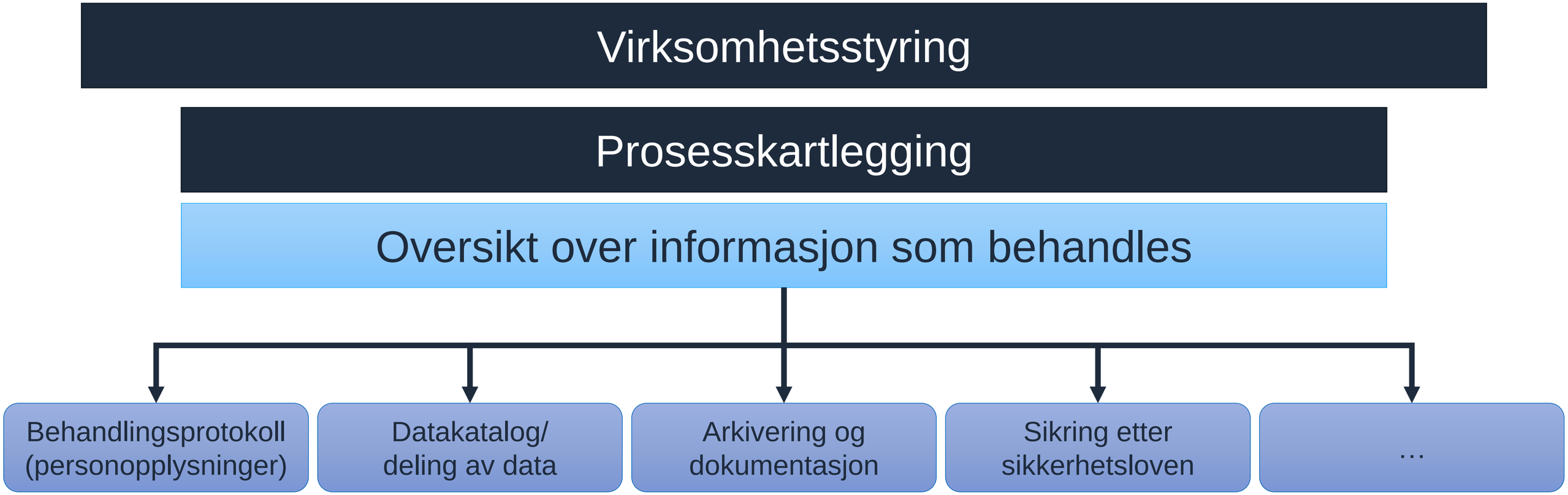
Vurdering av risiko

- Hold oversikt og prioritere
- De henter fra katalogen
  - 80% ferdig!
- Tilpasser og får oversikt over hva de driver med

Katalog

- oppgaver
- informasjonstyper
- utgangspunkt vurdering behov K-I-T


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


Virksomhetsstyring
Prosesskartlegging
Oversikt over informasjon som behandles
Behandlingsprotokoll (personopplysninger)
Datakatalog/ deling av data
Arkivering og dokumentasjon
Sikring etter sikkerhetsloven
…

Leveranser og tidsplan

Hovedleveranser

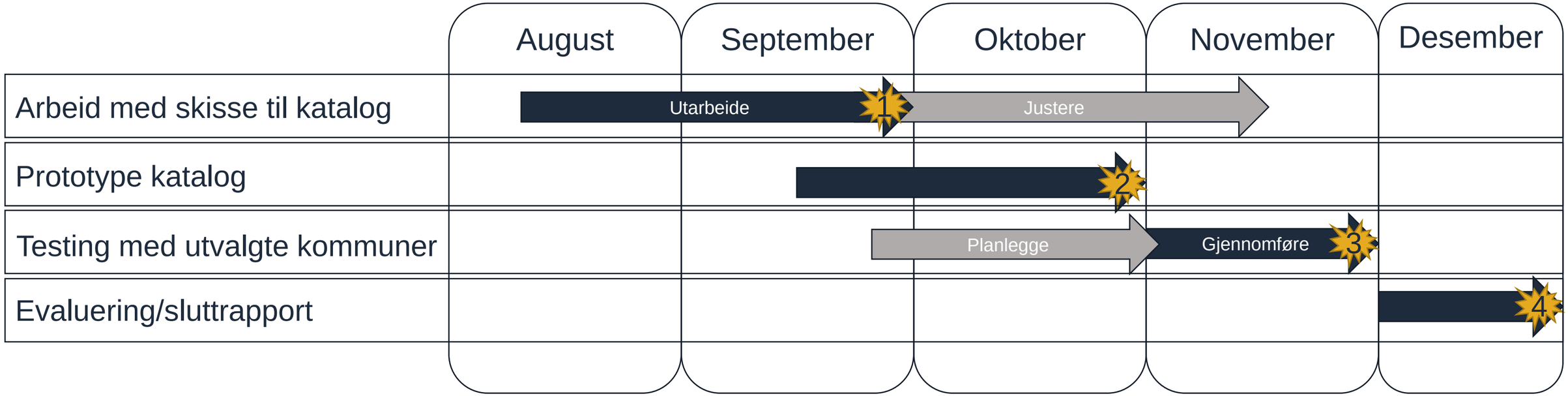
- Beskrivelse av utforming av katalog
- Utarbeide og teste prototype av katalog
- Sluttrapport – evaluering, veien videre

Digdir

digdir.no

Høsten 2022

1 Utkast til katalog klart
2 Prototype klar til testing
3 Testing gjennomført
4 Sluttrapport ferdig



Spørsmål?

Til diskusjon 1

Hvordan arbeider din virksomhet med å få oversikt over oppgaver og tjenester (herunder informasjon i disse)?

- Hvilke positive erfaringer har dere fra dette arbeidet?
- Hva har vært utfordrende i dette arbeidet?
- Hvis tid: Hvilke oversikter har dere allerede – på andre/tilgrensende områder? Kan noe gjenbrukes?

25 minutter diskusjon + 10 min plenum

Til diskusjon 2

Hvordan bør en katalog over oppgaver, tjenester og informasjonstyper utformes for å passe inn i din virksomhet?

- Hvilke områder (i din virksomhet) tenker du det er mest utfordrende å få oversikt over?
- Hvilke tjenester/oppgaver (hos dere) er hensiktsmessige å ta utgangpunkt i?
- Hvilke gevinster vil en virksomhet kunne ha ved å ta i bruk en slik katalog over oppgaver og informasjonstyper?

25 minutter diskusjon + 10 min plenum

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