Digdir

digdir.no

God styring som også ivaretar nytt regelverk

2024-03-06 / Katrine Aam Svendsen / Digdir

NIS 2

EU direktiv

EØS-avtalen

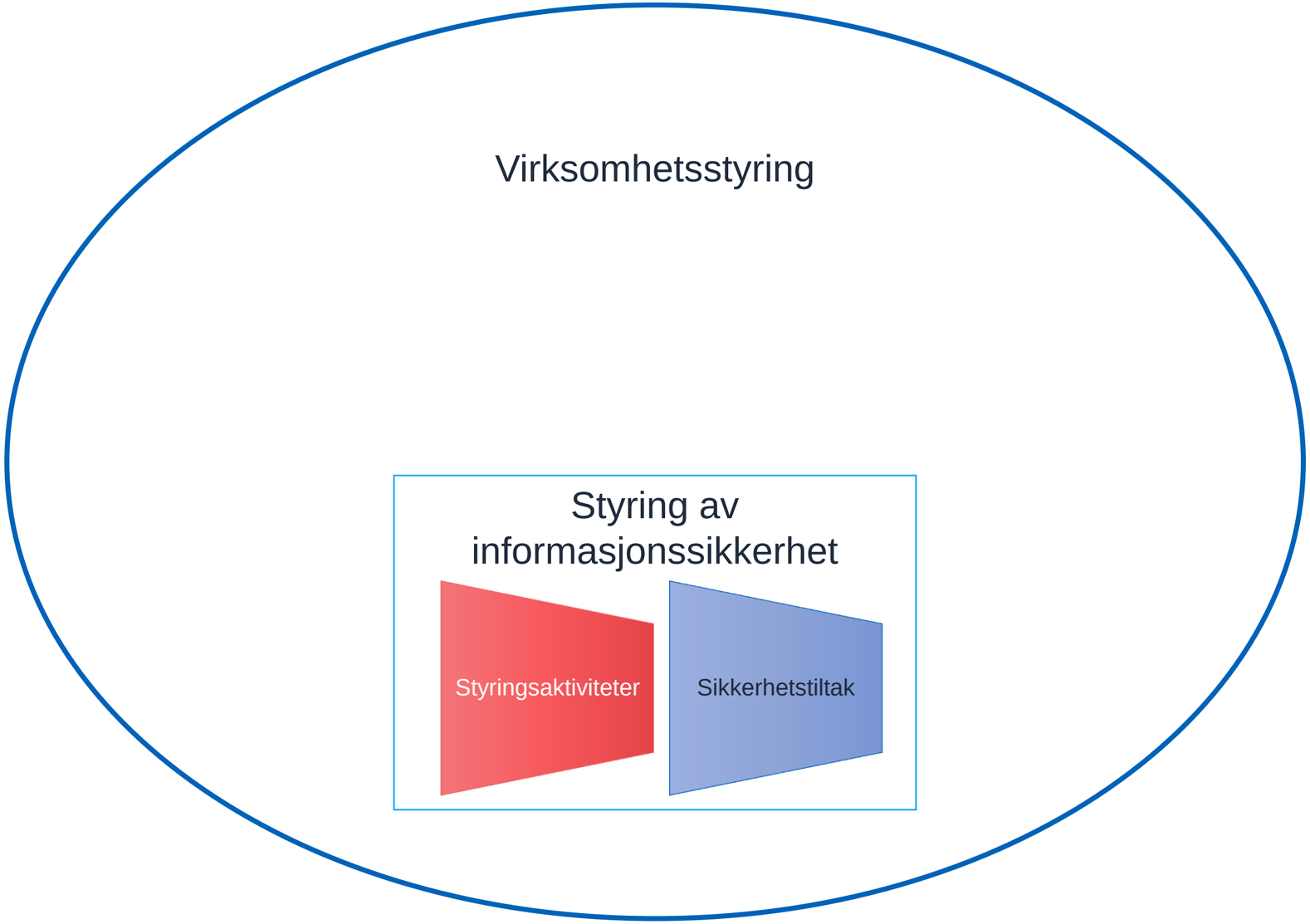
Stortinget

Norsk lov og forskrift

Pliktsubjekt i Norge

NIS 2

- Foreløpig ikke implementert i lov og forskrift i Norge
- Vi ser litt på direktivets minimumskrav til virksomheter
- Hovedsakelig artikkel 20, 21 og 23
- Med alle forbehold ☺


Virksomhetsstyring
Styring av informasjonssikkerhet
Styringsaktiviteter
Sikkerhetstiltak

Styringsaktiviteter

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

Sikkerhetstiltak

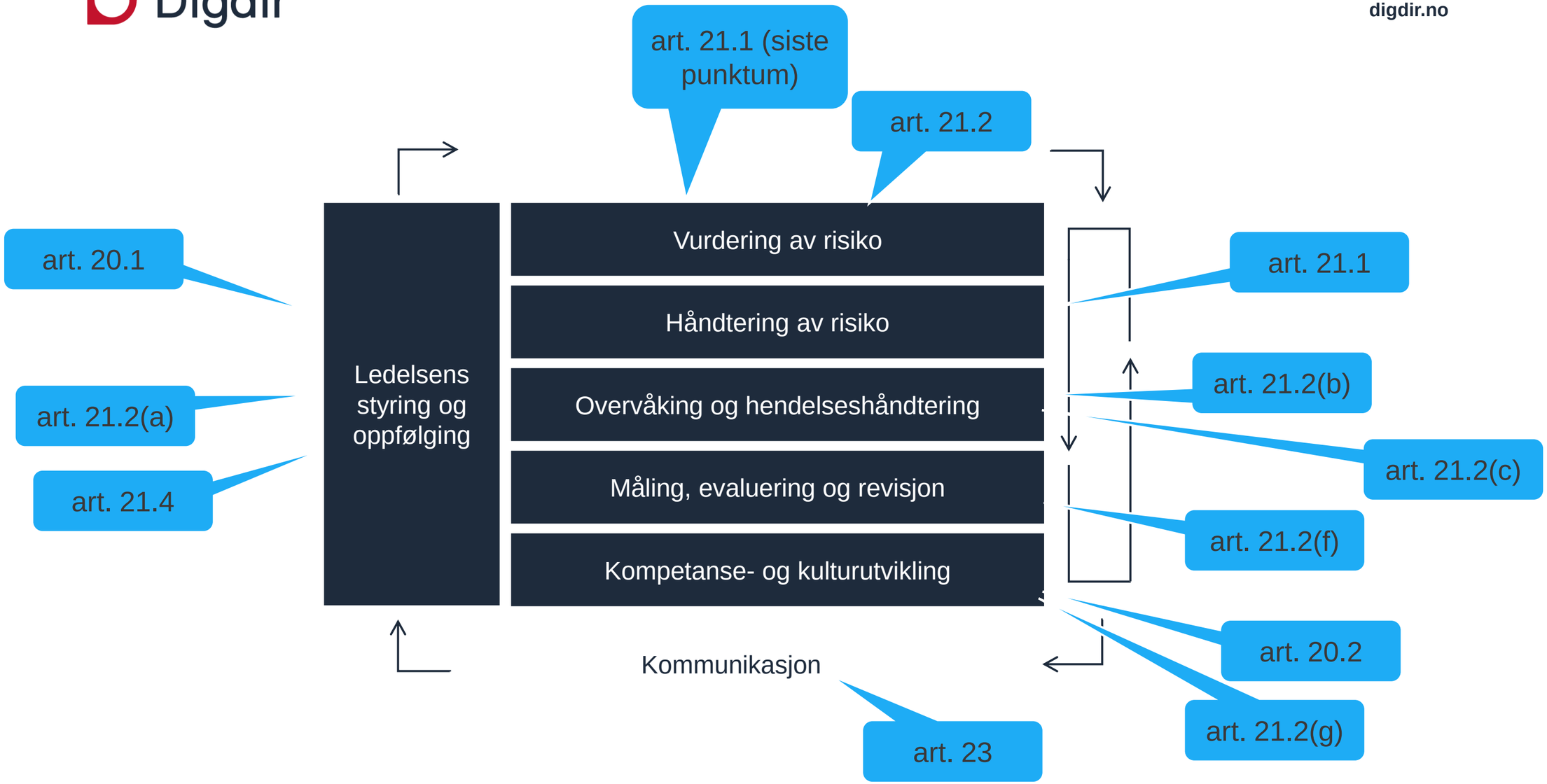
Formål

- Forebygge
- Oppdage
- Håndtere og gjenopprette

Typer

- Organisatoriske
- Menneskelige
- Fysiske
- Teknologiske


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


art. 21.1 (siste punktum)
art. 21.2
art. 20.1
art. 21.2(a)
art. 21.4
Ledelsens styring og oppfølging
Vurdering av risiko
Håndtering av risiko
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon
art. 21.1
art. 21.2(b)
art. 21.2(c)
art. 21.2(f)
art. 20.2
art. 21.2(g)
art. 23

NIS 2

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

art. 21.2(c)

art. 21.2(d)

art. 21.2(e)

art. 21.2(h)

art. 21.2(i)

art. 21.2(j)

Ledelsens styring og oppfølging

- management bodies
  - approve the cybersecurity risk-management measures
  - oversee its implementation
- policies on risk analysis and information system security
- an entity that finds that it does not comply [..] takes [..] all necessary, appropriate and proportionate corrective measures

Vurdering av risiko

- due account shall be taken of the degree of the entity’s exposure to risks, the entity’s size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact
- measures [..] shall be based on an all-hazards approach

Håndtering av risiko

- take appropriate and proportionate technical, operational and organisational measures
  - to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services
  - [..] to prevent or minimise the impact of incidents on recipients of their services and on other services

Overvåking og hendelseshåndtering

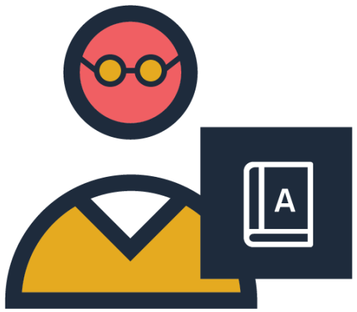
- incident handling
- crisis management

Måling, evaluering og revisjon

- assess the effectiveness of cybersecurity risk-management measures

Kompetanse- og kulturutvikling

- the members of the management bodies [..]
  - are required to follow training
  - shall encourage [..] similar training to their employees on a regular basis
- cybersecurity training



Kommunikasjon

- notify [..] its CSIRT or, where applicable, its competent authority
- notify [..] the recipients of their services of significant incidents
- communicate [..] to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat

Regelverk sett fra virksomhetenes perspektiv


Oppgaver
Tjenester

- Forvaltningsloven
- Sikkerhetsloven
- Personopplysningsloven
- Kommuneloven
- "Styringsregelverket" i staten
- Sektor-regelverk


Oppgaver
Tjenester
Forvaltningsloven
Sikkerhetsloven
Personopplysningsloven
Kommuneloven
"Styringsregelverket" i staten
Sektor-regelverk
Lov om digital sikkerhet

Digdir

NSM

Digdir

dfø

KS

Datatilsynet

Direktoratet for e-helse

Oppgaver
Tjenester

- Forvaltningsloven
- Sikkerhetsloven
- Personopplysningsloven
- Kommuneloven
- "Styringsregelverket" i staten
- Sektor-regelverk
- Lov om digital sikkerhet

NIS – informasjonssystem

(1) ‘network and information system’ means:

(a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

Sikkerhetsloven – informasjonssystem

- Utvalget legger til grunn en vid forståelse av begrepet informasjonssystem, jf. merknaden til utvalgets lovforslag § 6-1 i NOU 2016: 19, side 262:

- «Med begrepet informasjonssystem menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker. Informasjonssystem skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.»

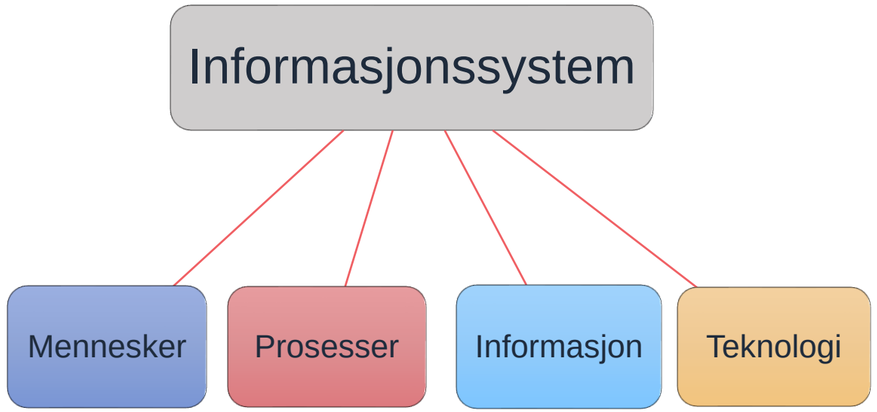
- Departementet stiller seg bak denne tilnærmingen og mener at beskrivelsen er dekkende for begrepet informasjonssystem.

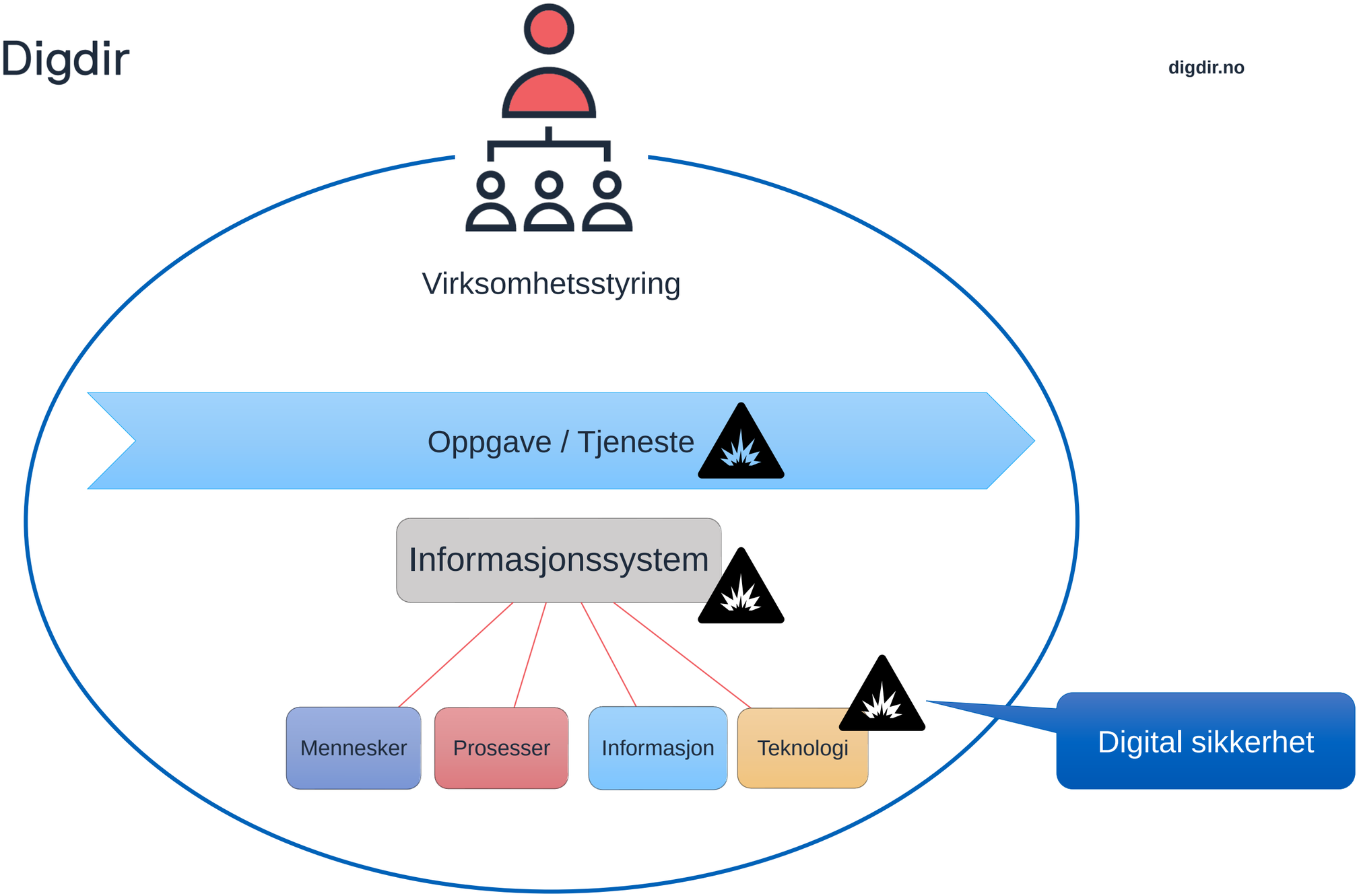
Prop. 153 L (2016 –2017), 10.5.3.1, s. 99

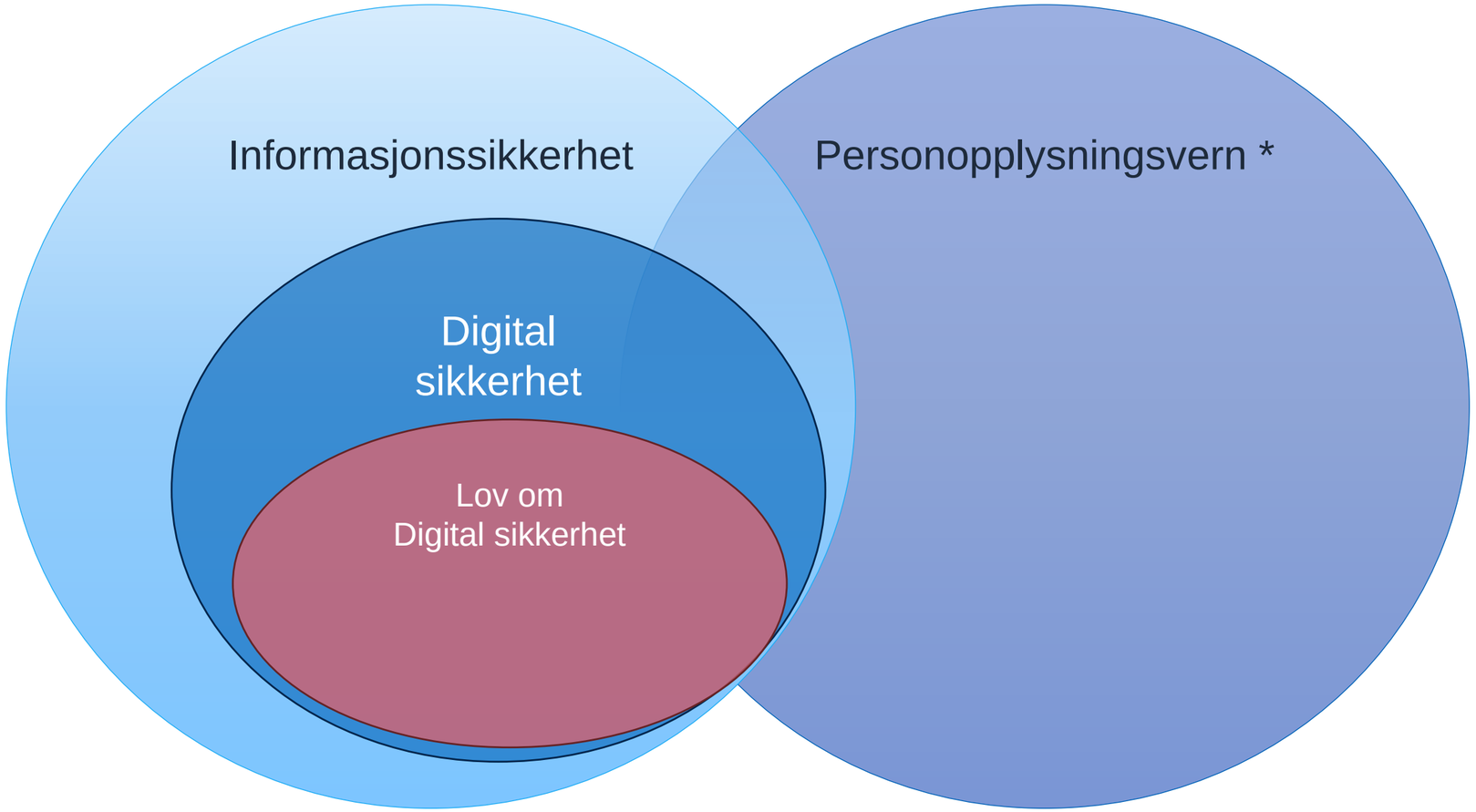
Informasjons(behandlings)sikkerhet

Styre risiko ved bruk av *informasjonssystemer* i oppgaveløsningen

Oppgave / Tjeneste

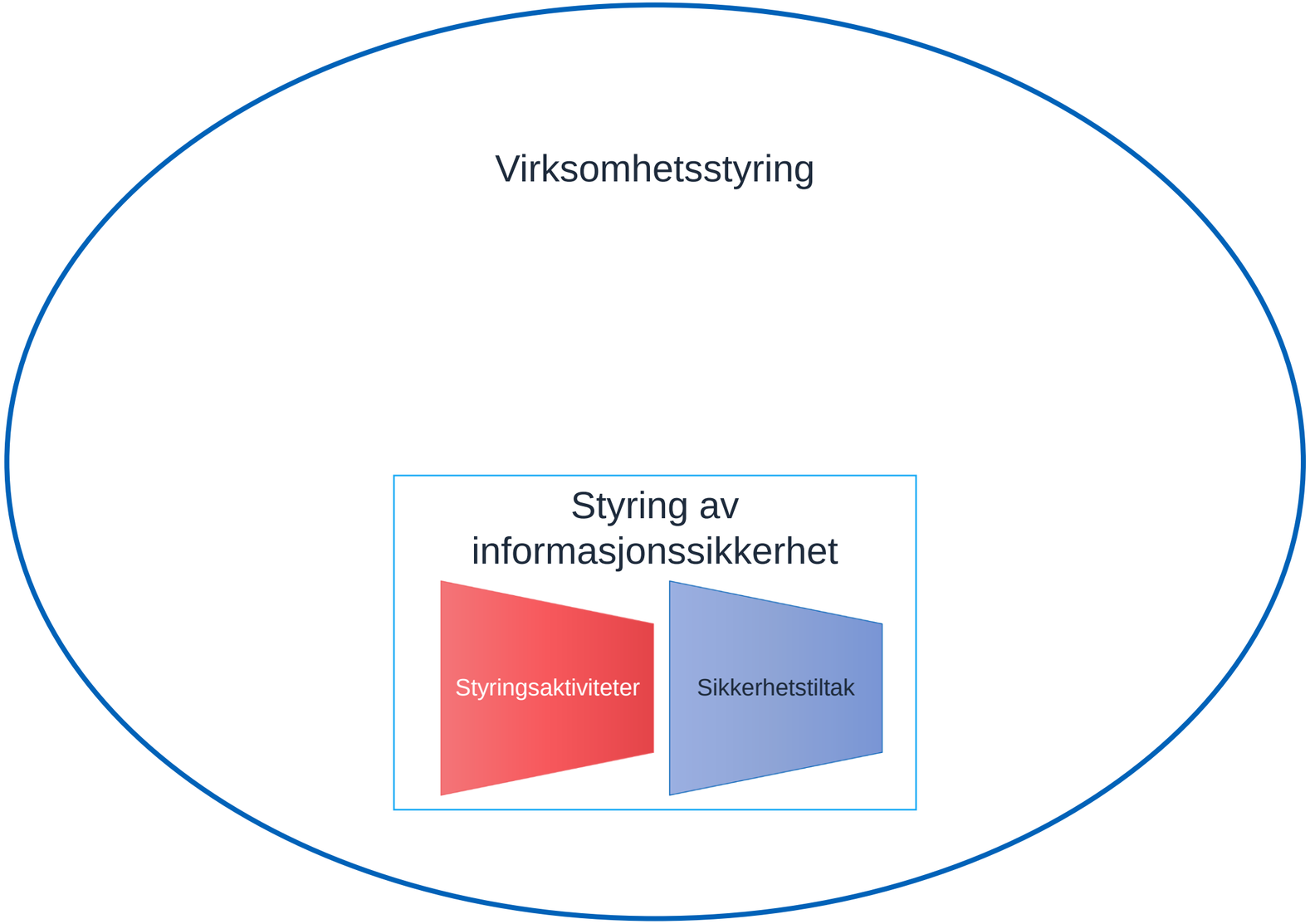



Virksomhetsstyring
Oppgave / Tjeneste
Informasjonssystem
Mennesker
Prosesser
Informasjon
Teknologi
Digital sikkerhet



* Vi tenker her hovedsakelig på virksomhetenes plikter iht. pvf kap. IV

Arbeide helhetlig med disse tingene


Virksomhetsstyring
Styring av informasjonssikkerhet
Styringsaktiviteter
Sikkerhetstiltak

Digitaliseringsrundskrivet

Rundskriv | Dato: 21.12.2022

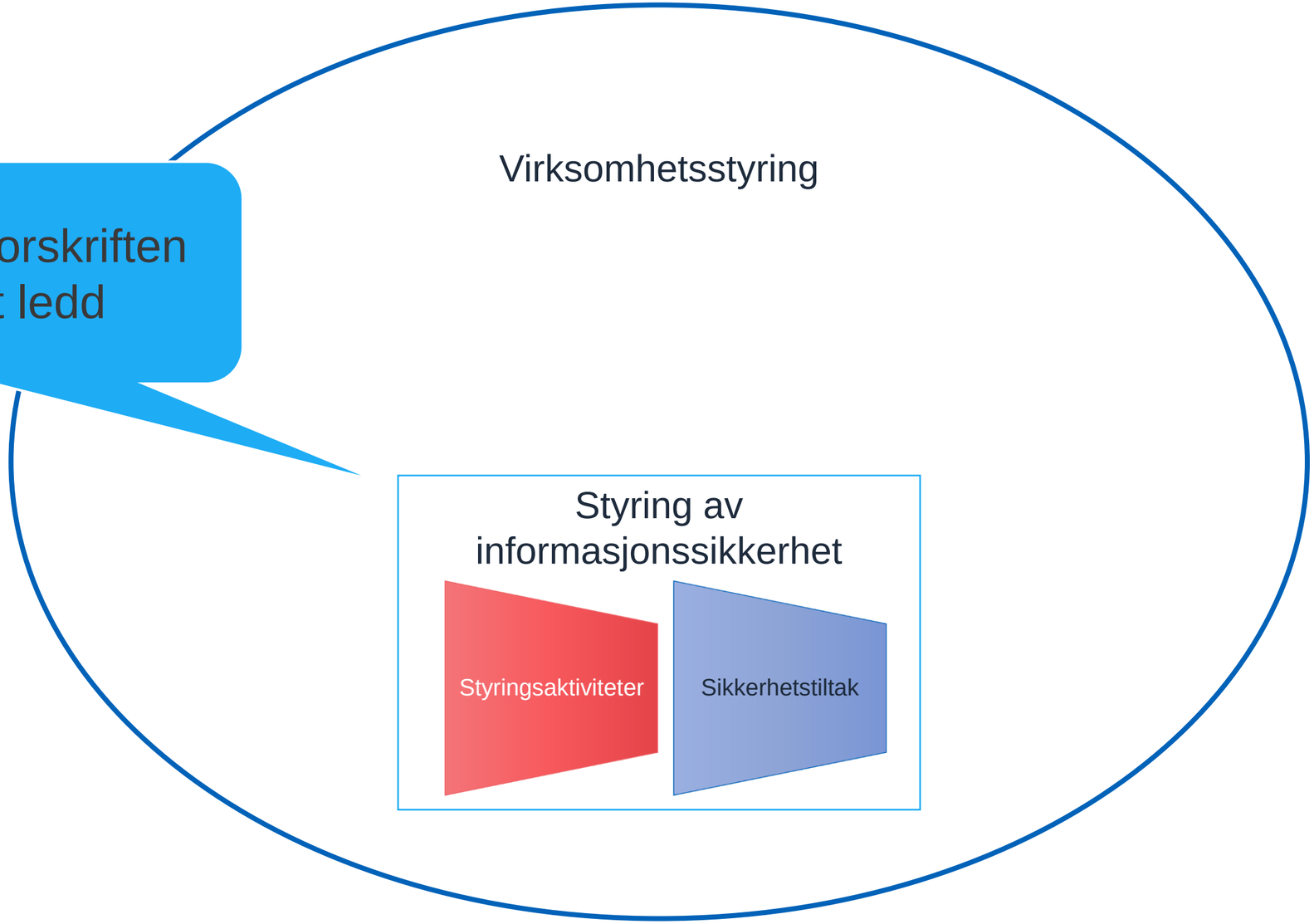
Krav

I henhold til eForvaltningsforskriften § 15 skal virksomheten ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Omfang og innretning på internkontrollen skal være tilpasset risikoen.

Anbefaling

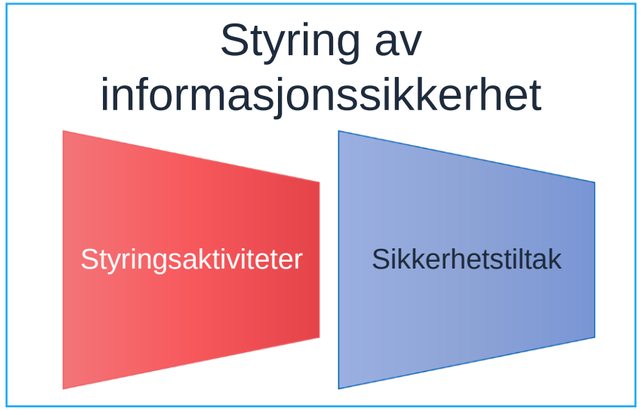
KDD har pekt ut Digitaliseringsdirektoratet til det organ som skal gi anbefalinger om internkontroll (styring og kontroll) på informasjonssikkerhetsområdet, jf. eForvaltningsforskriften § 15. En veileder finnes på Digitaliseringsdirektoratets nettsider. Denne veilederen understøtter virksomhetsledelsens arbeid med helhetlig internkontroll, blant annet ved å hjelpe virksomheten til å identifisere plikter etter annet regelverk, som personvernforordningen. (jf. nedenfor pkt 1.5).

eForvaltningsforskriften
§ 15 annet ledd



eForvaltningsforskriften
§ 15 annet ledd

Virksomhetsstyring

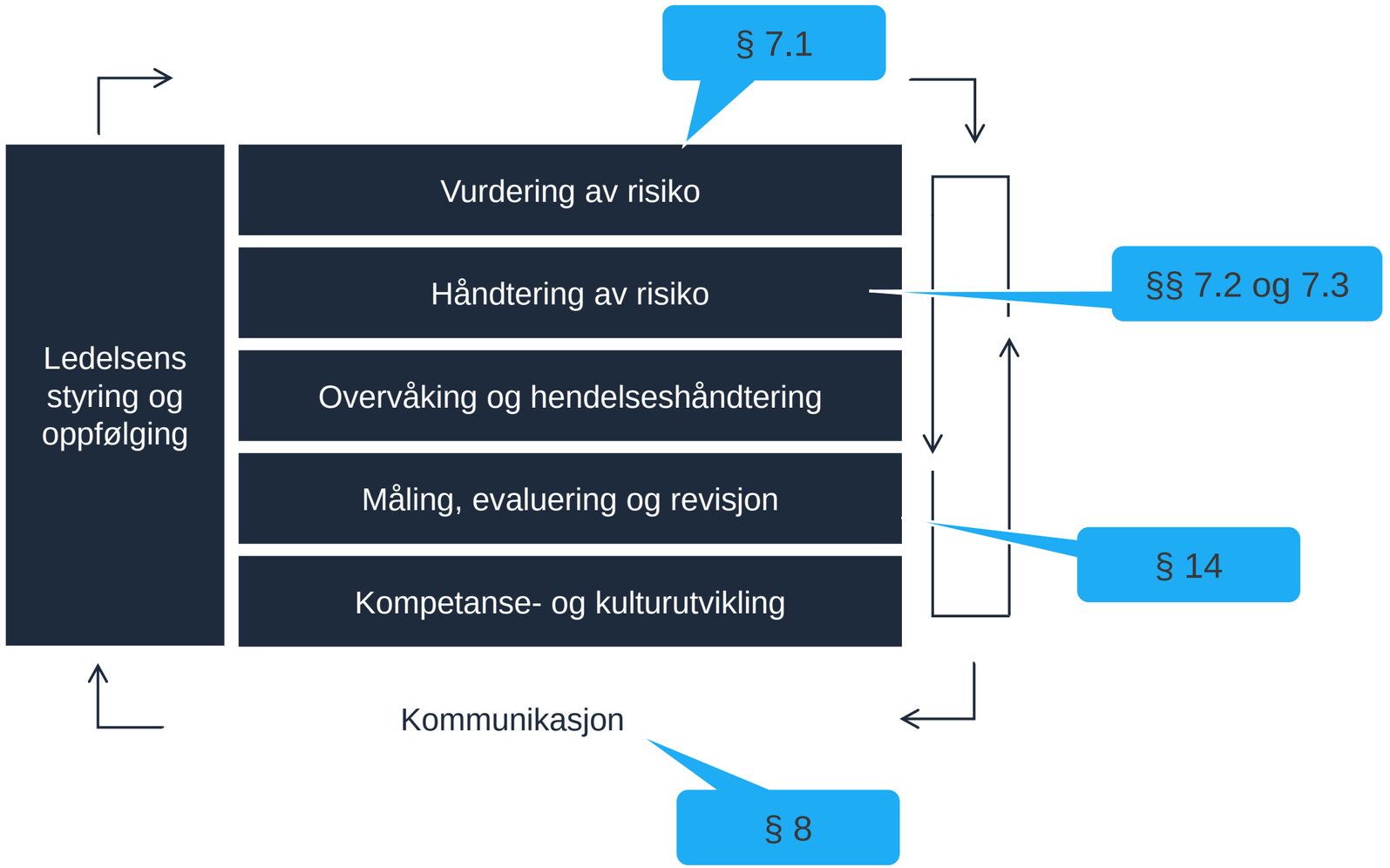


styring og kontroll på informasjonssikkerhetsområdet

som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet

en integrert del av virksomhetens helhetlige styringssystem

skal inkludere relevante krav i annen lov, forskrift eller instruks



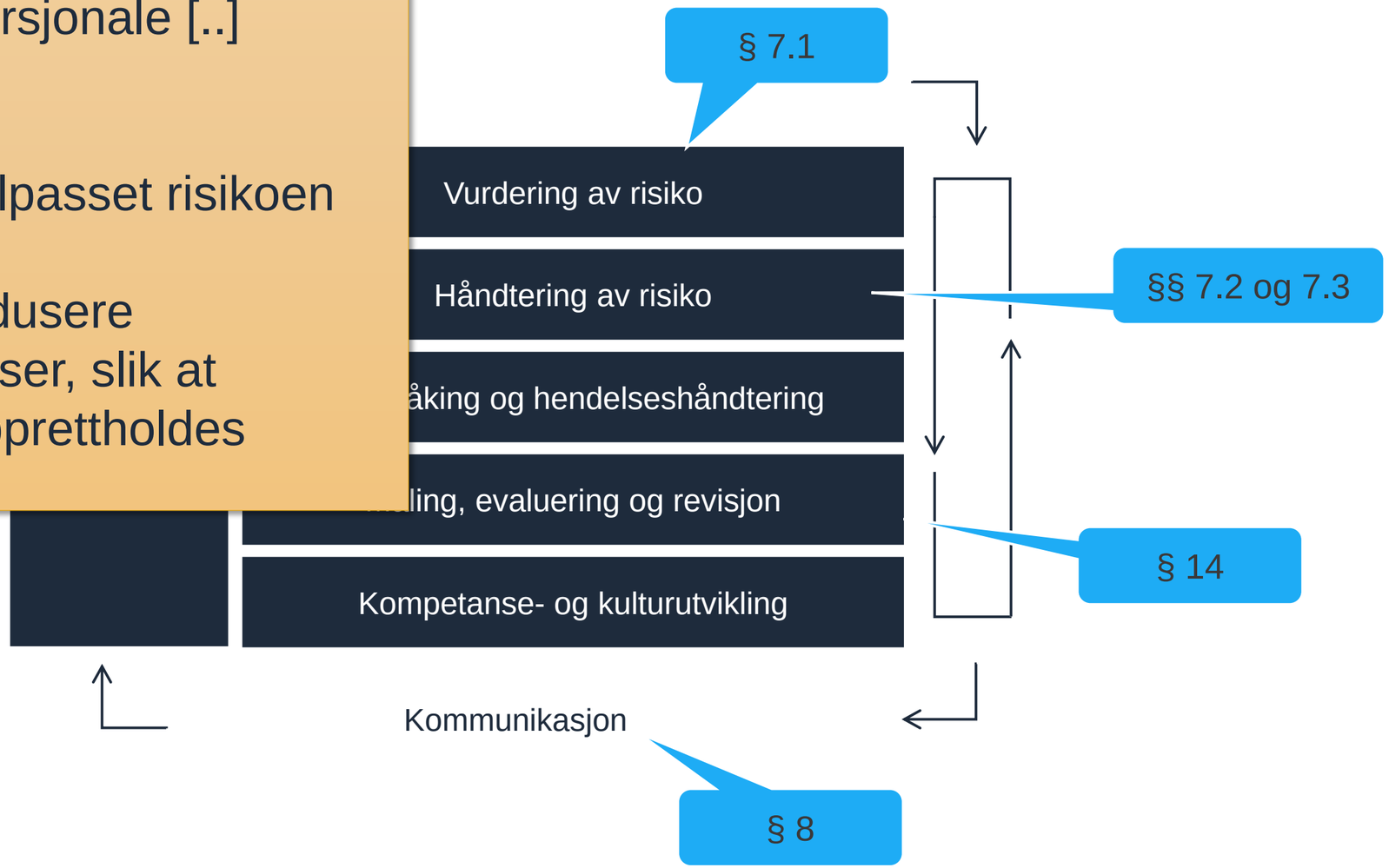
Lov om digital sikkerhet

risikovurdering av nettverks- og informasjonssystemer

hensiktsmessige og proporsjonale [..] sikkerhetstiltak

et sikkerhetsnivå som er tilpasset risikoen

forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes

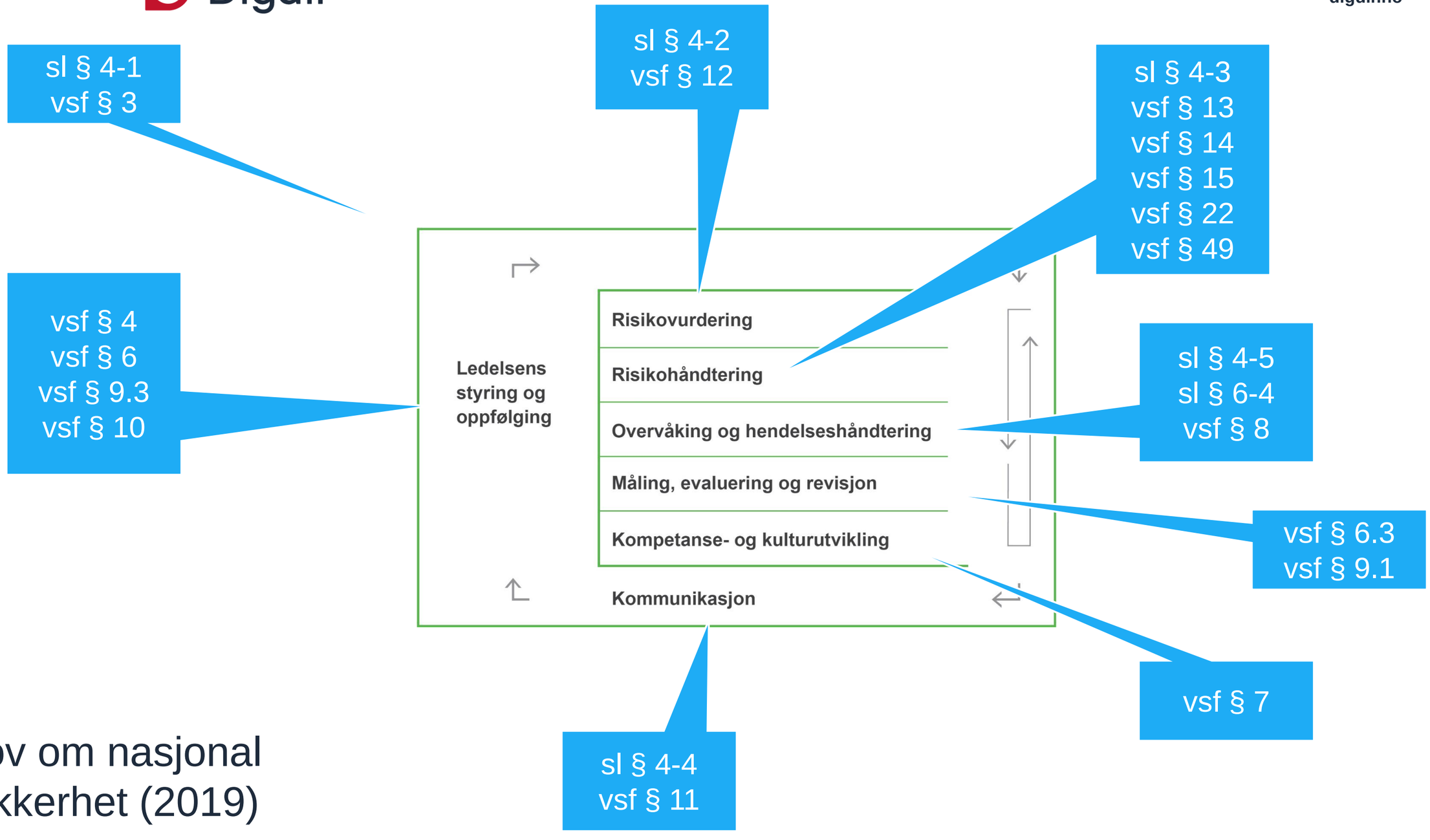


Lov om digital sikkerhet

Digdir

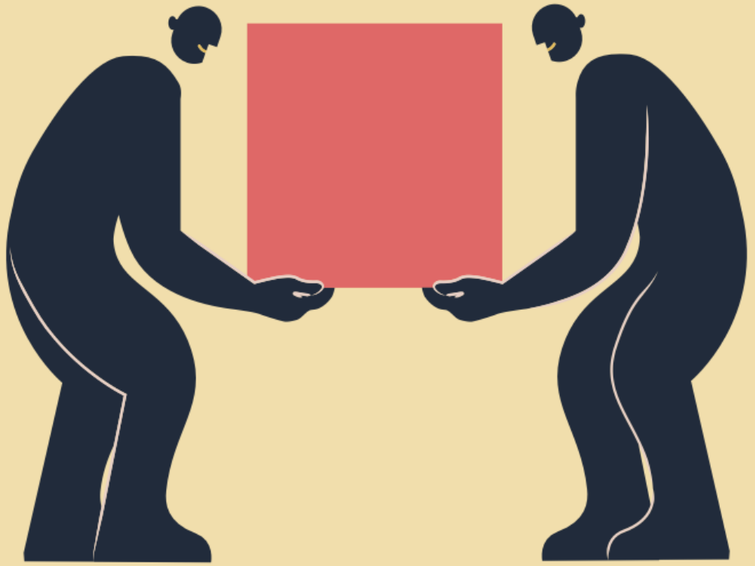
digdir.no

Lov om nasjonal sikkerhet (2019)



Helhetlig styring og kontroll av informasjonssikkerhet

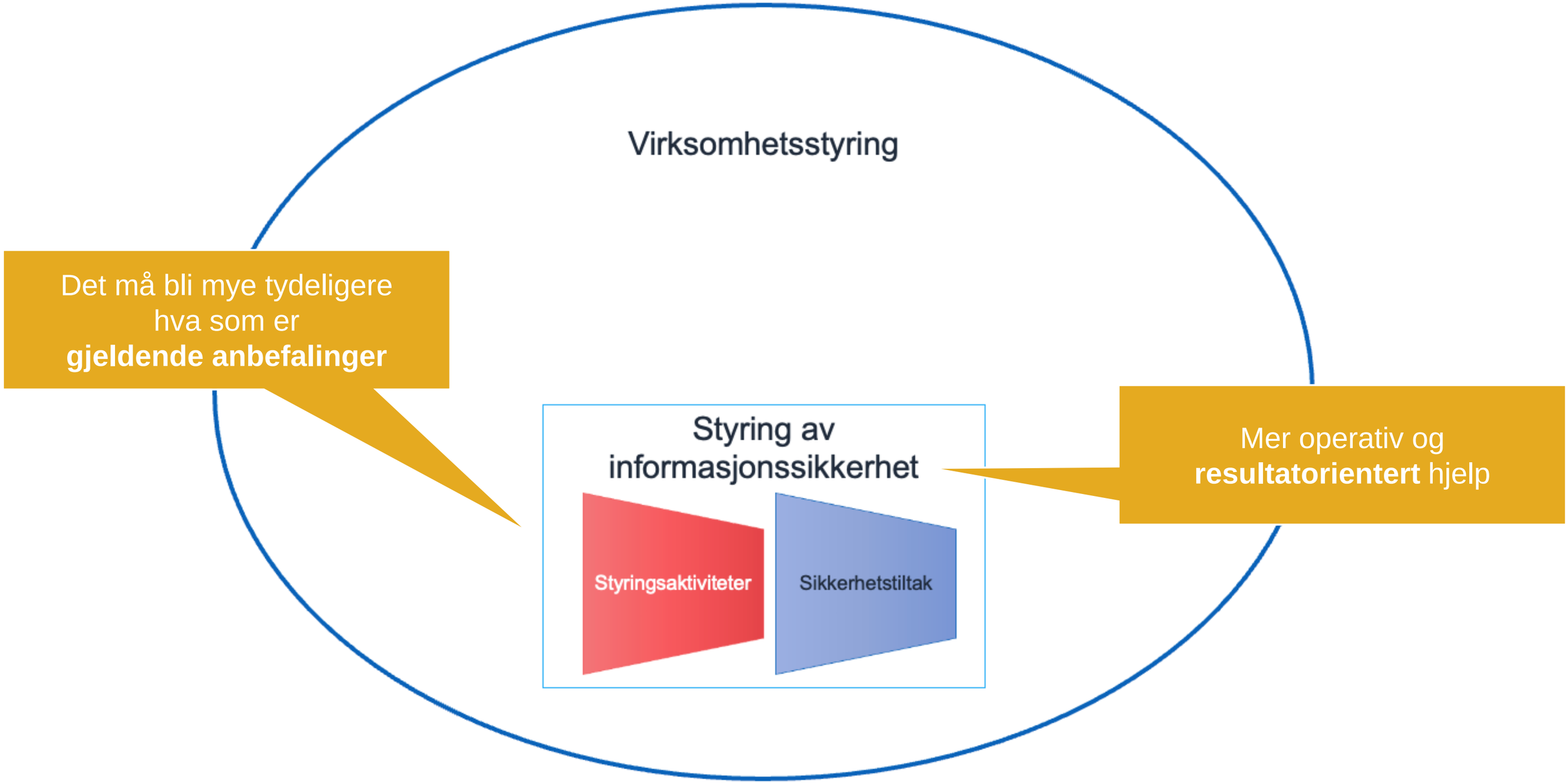
For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



digdir.no

Felles sikkerhet i forvaltningen


NSM
Data-
tilsynet
JD
Sektor-
departement
UD
FD
Sektor
etat
Andre
departe-
menter
Difi
Sektorvis
respons-
miljø
Nkom
SD
DSB
KMD
Sektortilsyn


Virksomhetsstyring
Det må bli mye tydeligere hva som er **gjeldende anbefalinger**
Styring av informasjonssikkerhet
Styringsaktiviteter
Sikkerhetstiltak
Mer operativ og **resultatorientert** hjelp

KS

NSM

HDir

Datatilsynet

Økonomireglementet i staten

Digdir

DFØ

Personopplysningsloven

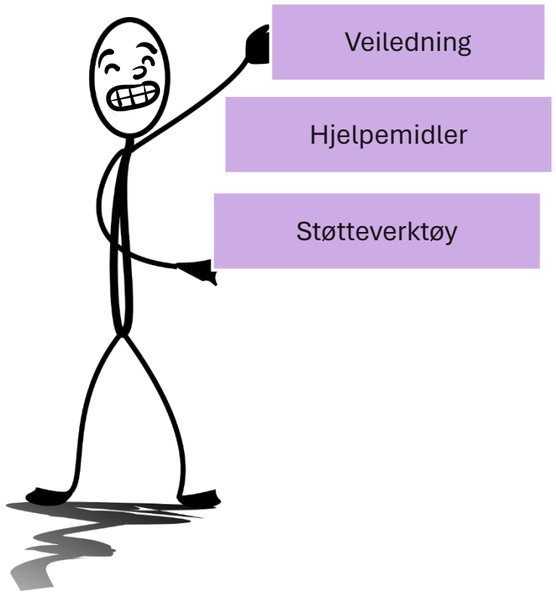
Sikkerhetsloven

eForvaltningsforskriften § 15.2

Kommuneloven

Digitalsikkerhetsloven

Felles anbefalinger

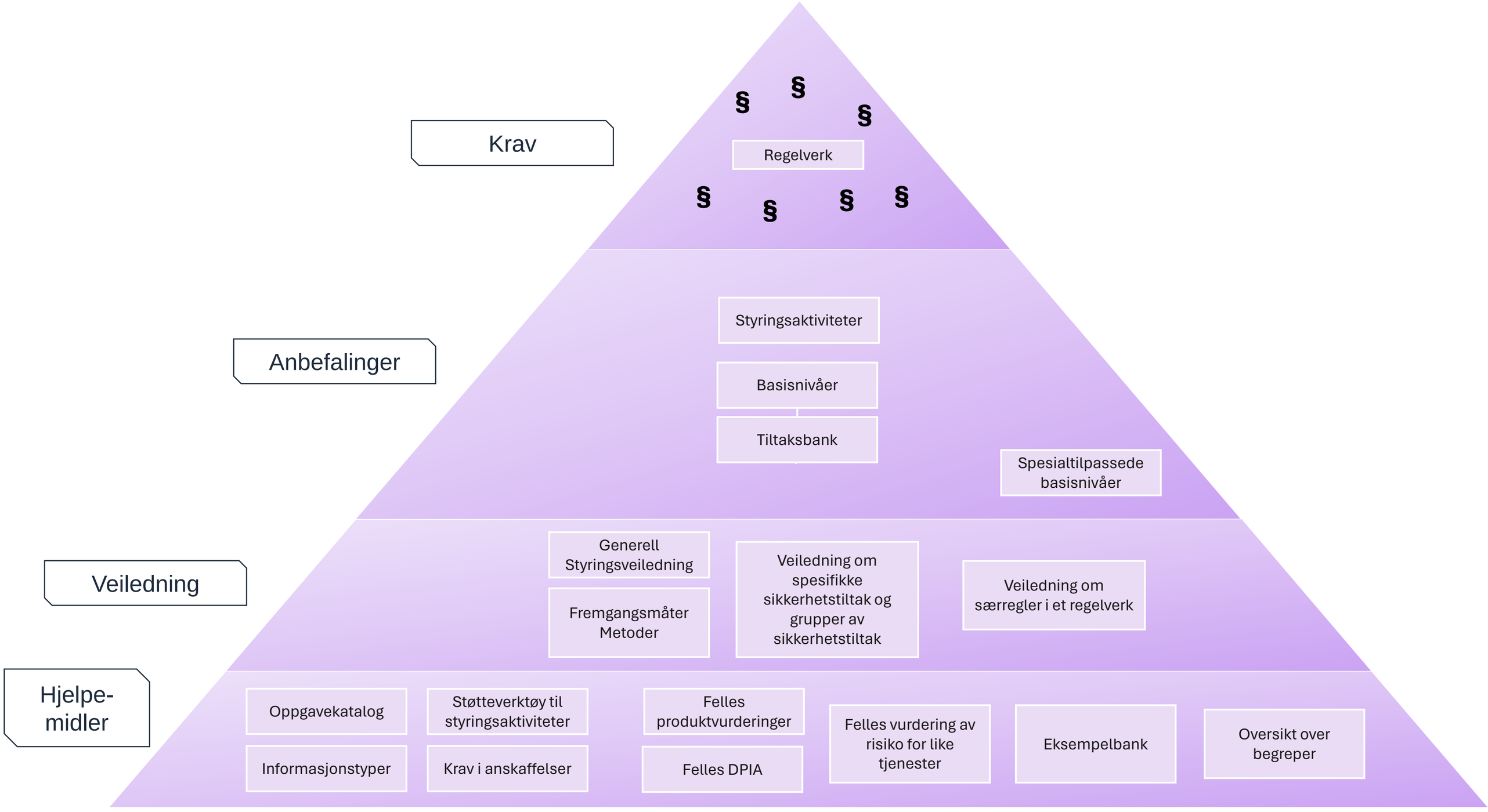


Veiledning

Hjelpemidler

Støtteverktøy

- Publisert desember 2022
- Sammen med innspill fra statlige og kommunale aktører


Krav
§ § § § § §
Regelverk
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Veiledning
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Hjelpe-midler
Oppgavekatalog
Støtteverktøy til styringsaktiviteter
Informasjonstyper
Krav i anskaffelser
Felles produktvurderinger
Felles DPIA
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper

Til slutt

Digdirs veiledning

- Vil bli oppdatert med informasjon om lov om digital sikkerhet m/forskrifter
- https://digdir.no/ik

Spørsmål?

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