Hvilke konsekvenser får NIS2 for myndigheter og virksomheter?

18. mars 2024

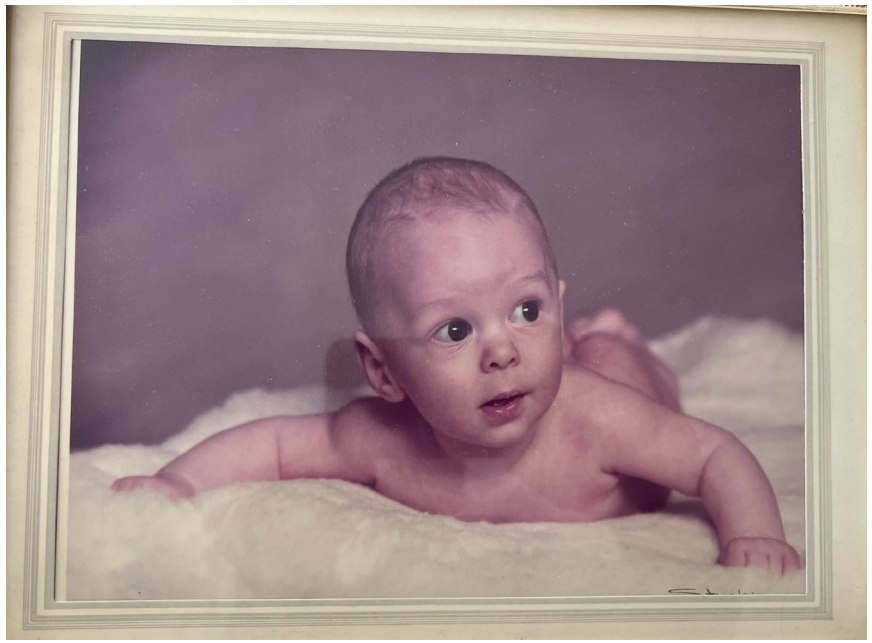
Medlemsmøte i Norsk Forening for Jus & EDB

Advokat Jens Christian Gjesti

KVALE

Hvorfor står jeg her i dag?

FASE 1



FASE 2

FASE 3

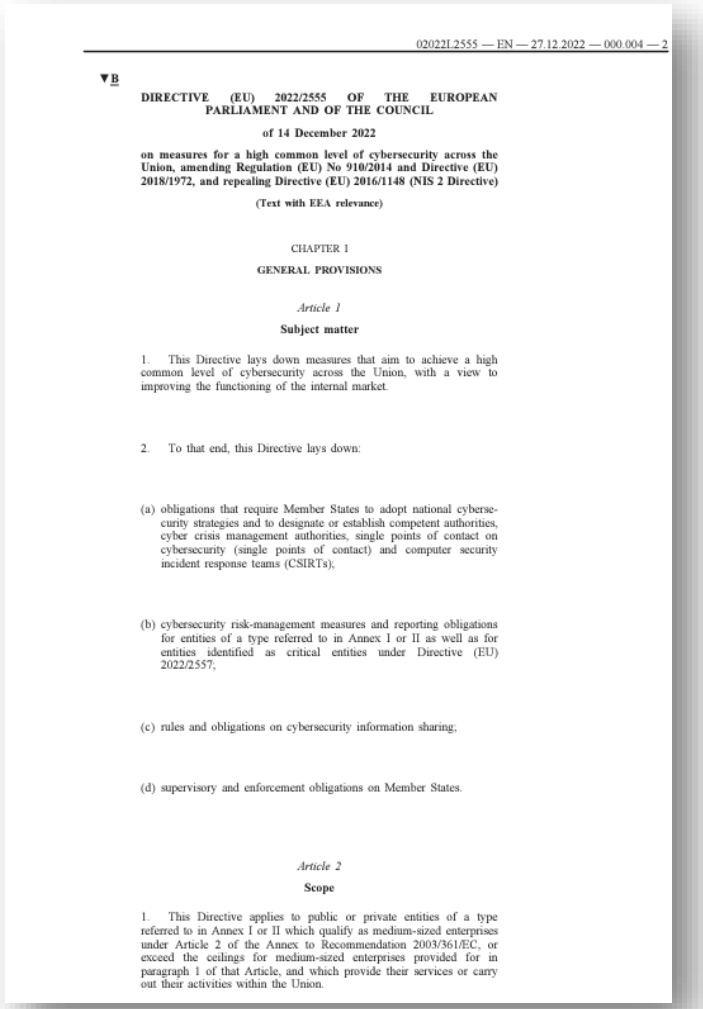
KVALE

Hva skal jeg snakke om i dag?

=

KVALE

Hva er målet mitt?



02022L2555 — EN — 27.12.2022 — 000.004 — 2

▼B

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

2. To that end, this Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;

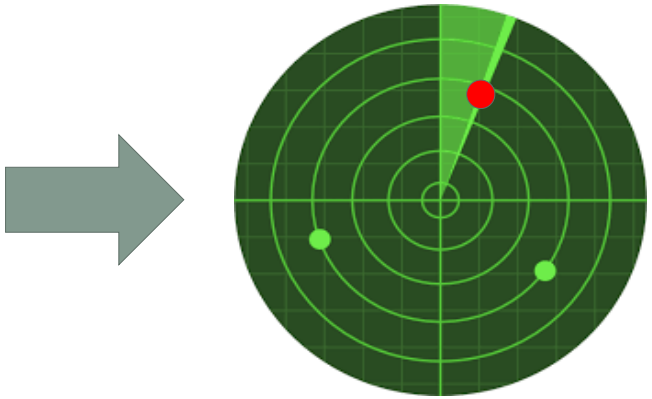
(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.



KVALE

Agenda

1. Utgangspunkt og knagger
2. Hva er NIS2?
3. Når, hvem og hvor?
4. Hvilke konsekvenser får NIS2?
    a) For offentlig og privat virksomhet?
    b) For lovgiver og tilsynsmyndighet?
5. Råd og tips på veien
6. Spørsmål

To og to – 5 min.

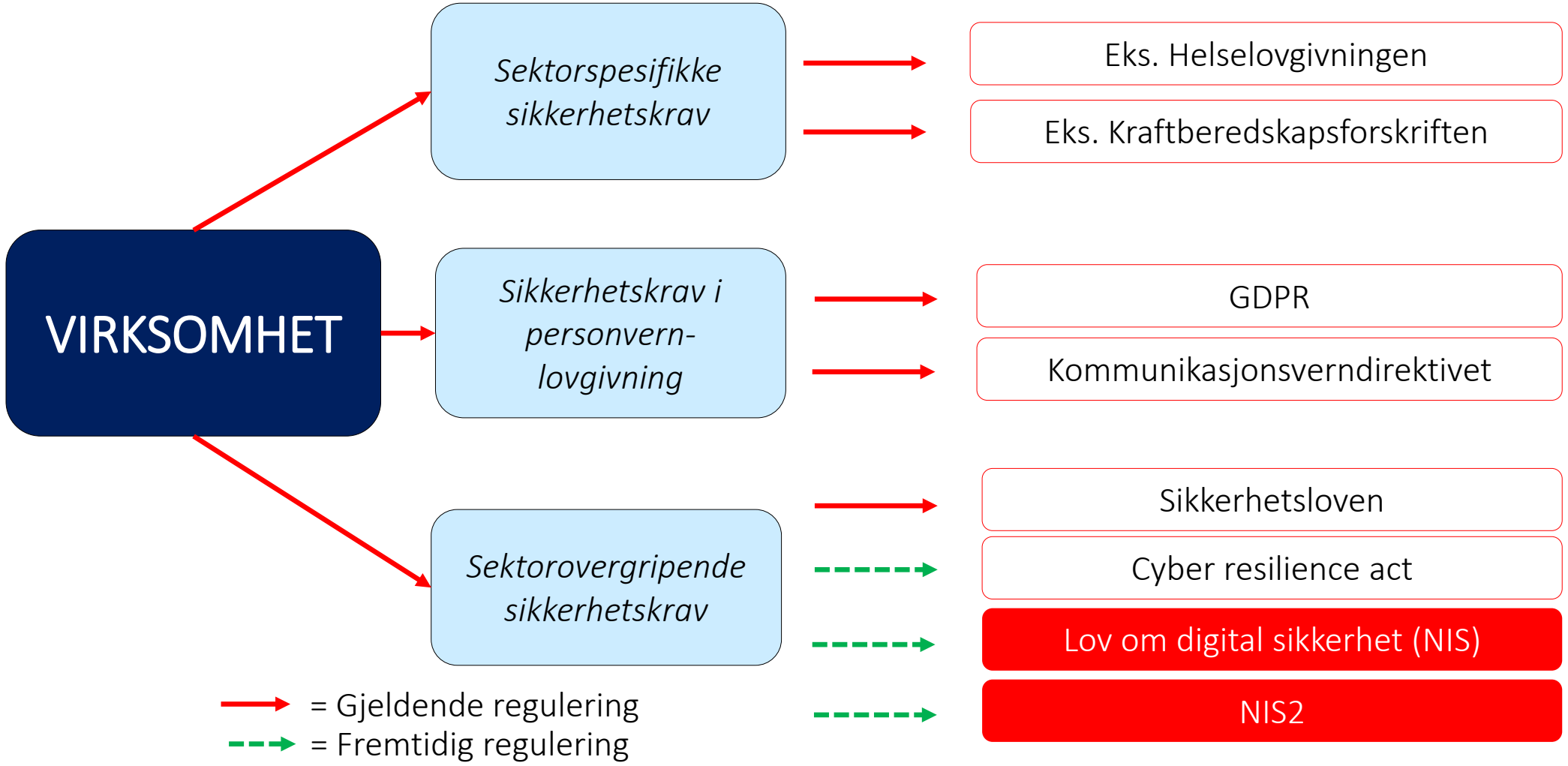
1. Hvem er du?
2. Hva vet du om NIS2?
3. Hva har du lyst til å høre mer om i dag?

1. Utgangspunkt og noen viktige knagger

Det finnes ikke én felles "cybersikkerhets-regulering"

KVALE

Ulike "typer" sikkerhetsregulering snakker sjeldent sammen



Hva er [x]sikkerhet?

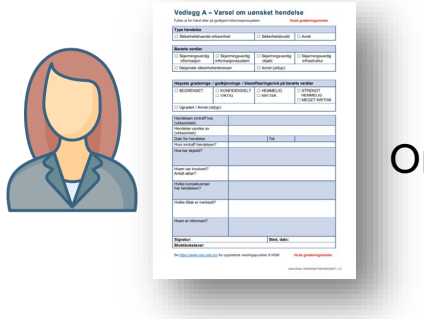
1. Beskyttelse av ulike verdier

2. Mot interne og eksterne trusler

3. Ved hjelp av risikobaserte tiltak

Microsoft Active Directory

Tekniske



Organisatoriske

Fysiske

KVALE

Til 1) Er "Cybersikkerhet" det samme som "informasjonssikkerhet"?

Morten Irgens

Hverdager er de flotteste. De er fulle av eventyr.

Om meg

Cybersikkerhet er ikke informasjonssikkerhet er ikke IKT-sikkerhet

July 27, 2013 Uncategorized

Informasjonssikkerhet, cybersikkerhet, datasikkerhet, IT-sikkerhet, IKT-sikkerhet, datasikkerhet – betyr alt dette det samme?

Nei, det gjør det ikke, selv om begrepene ofte, eller skal vi si som regel, brukes om hverandre. Jeg skal her gi mitt syn på hva begrepene betyr, og jeg tror det er konsistent med et nytt paper av von Solms and van Niekerk (2013).

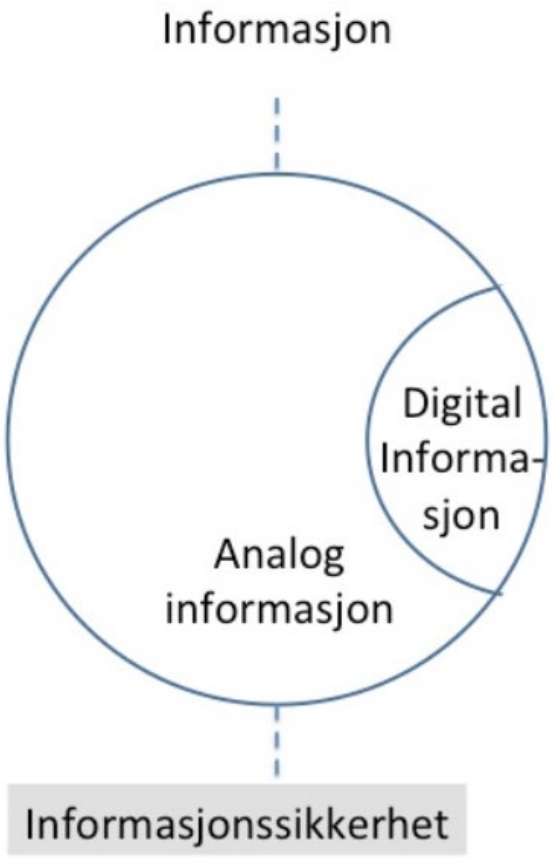
Noe av dette er enkelt å forstå. Informasjonssikkerhet har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke. IKT-sikkerhet har med sikring av Informasjons- og kommunikasjonsteknologi å gjøre – altså maskinvare og programvare. Grunnen til at IKT-sikkerhet og informasjonssikkerhet ofte blir brukt om hverandre, er nok at mye informasjon er lagret og formidlet ved hjelp av IKT. For å beskytte slik informasjon, må man beskytte teknologien den er lagret og formidlet på.

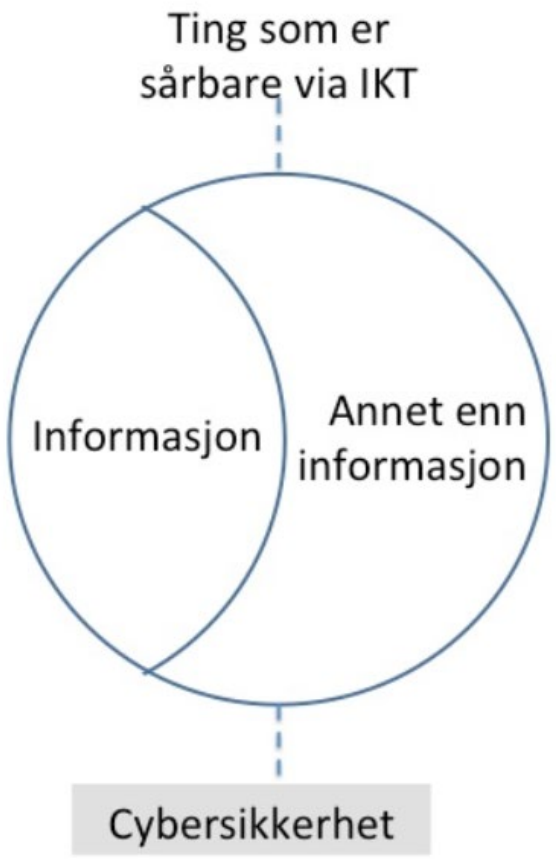
IT-sikkerhet har med sikring av informasjonsteknologi. I praksis er det ingen forskjell på IKT-sikkerhet og IT-sikkerhet.

KVALE

Kilde: "From information security to cyber security", Solms and van Niekerk, 2013: https://profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

Hva er "cybersikkerhet"?

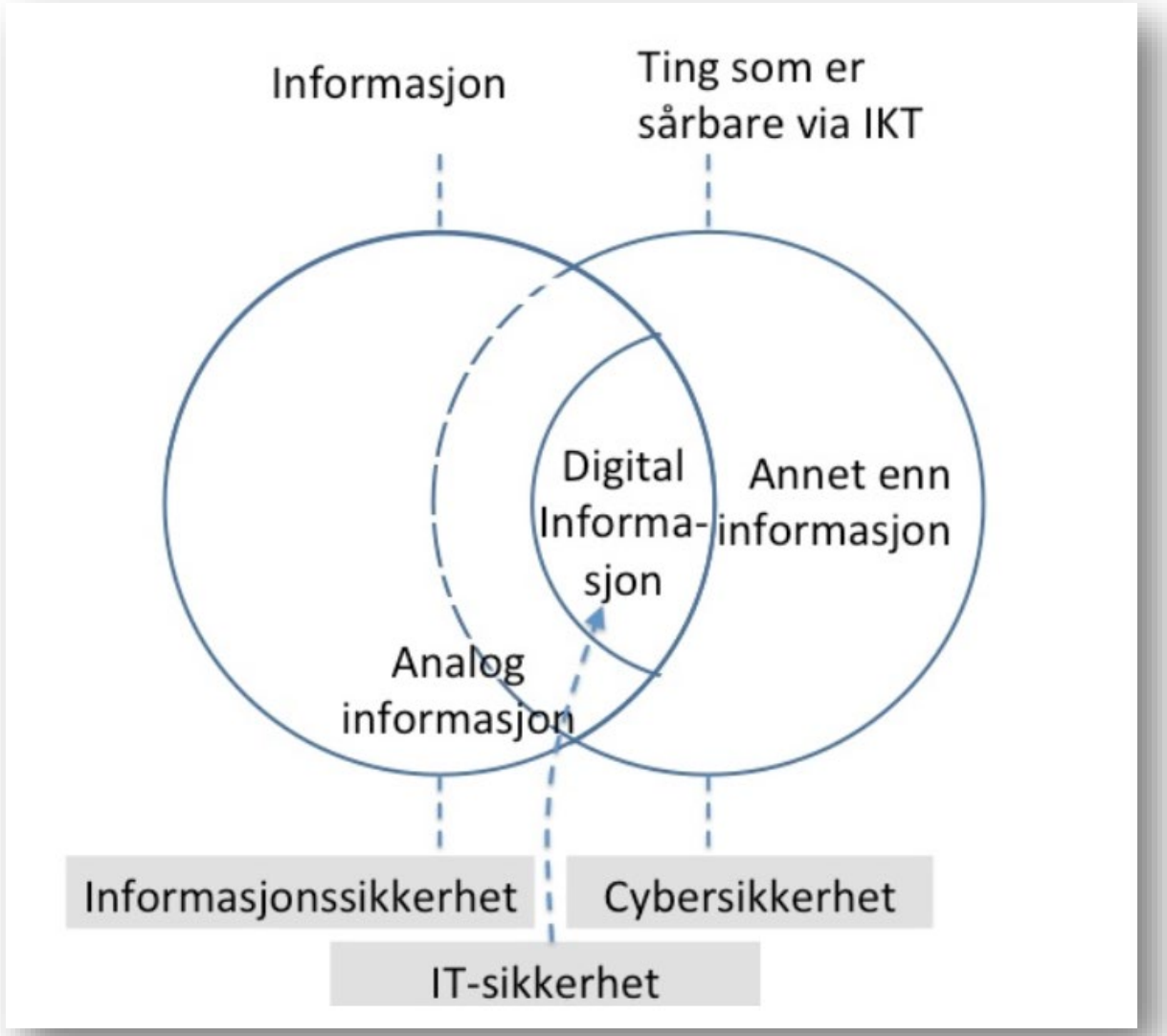




KVALE

http://mortenirgens.com/?p=769

Hva er "cybersikkerhet"? (forts.)



"Informasjonssikkerhet": Innholdet som overføres i et mobilnett slik som SMS, samtaler og IP-trafikk

"IT-sikkerhet": Informasjons- og kommunikasjonsteknologien, programvare og maskinvare

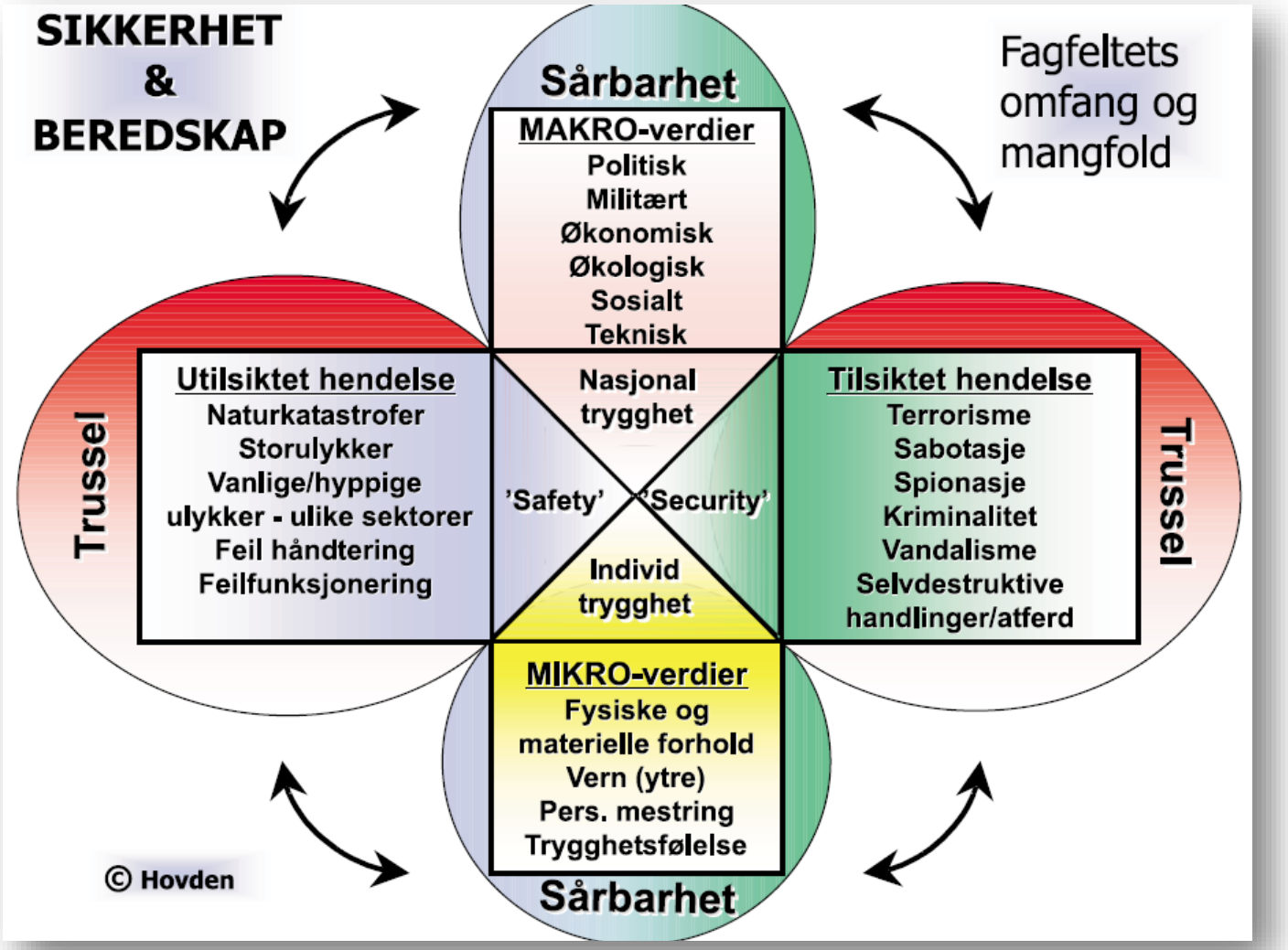
"Cybersikkerhet": Den logiske og fysiske ekominfrastrukturen slik som basestasjoner, transmisjon og mobile core og dataene i den

KVALE

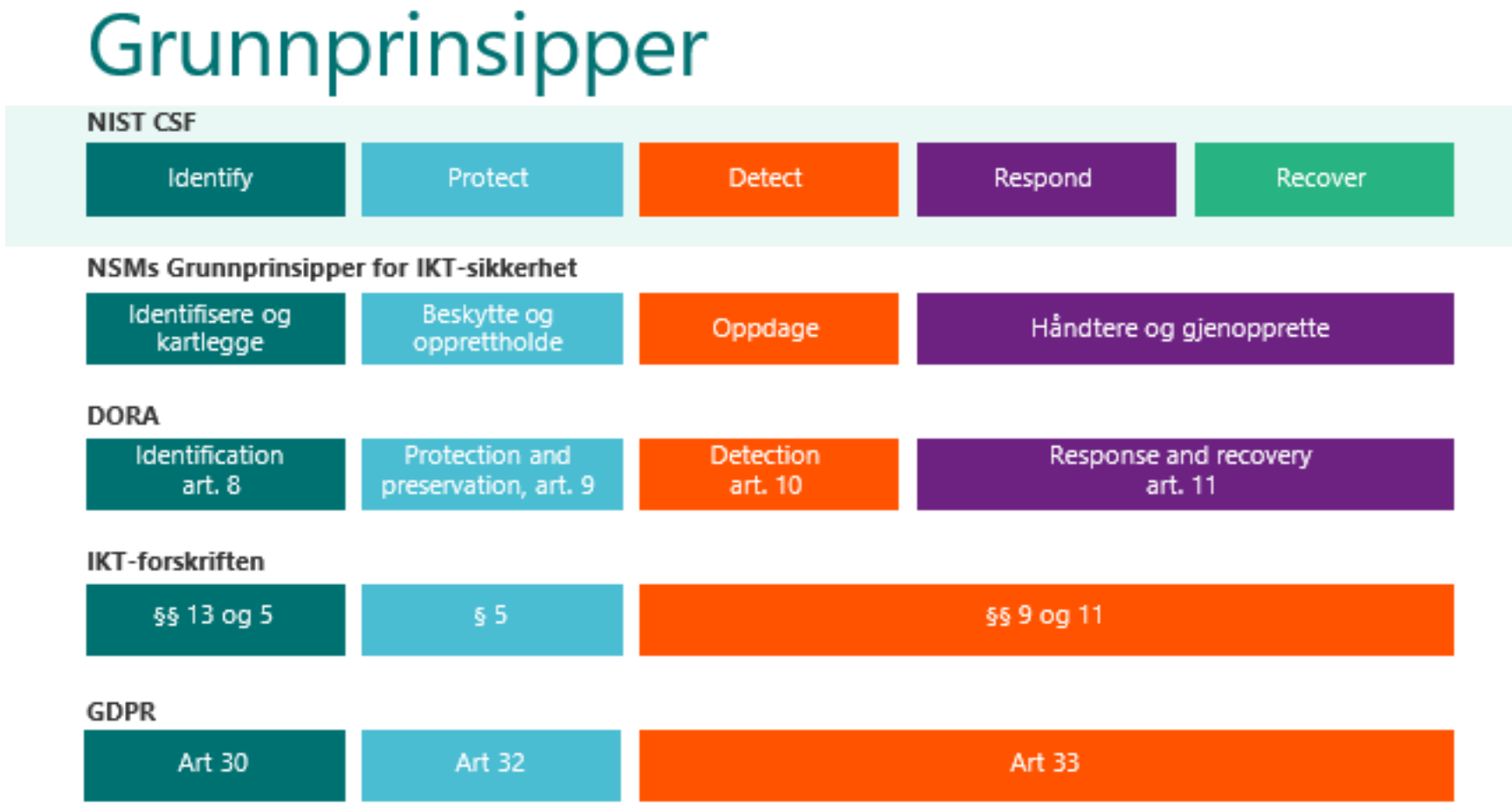
http://mortenirgens.com/?p=769

Til 2: "Sikkerhet" er noe annet enn "sikkerhet"..

"Safety, safety, safety!"



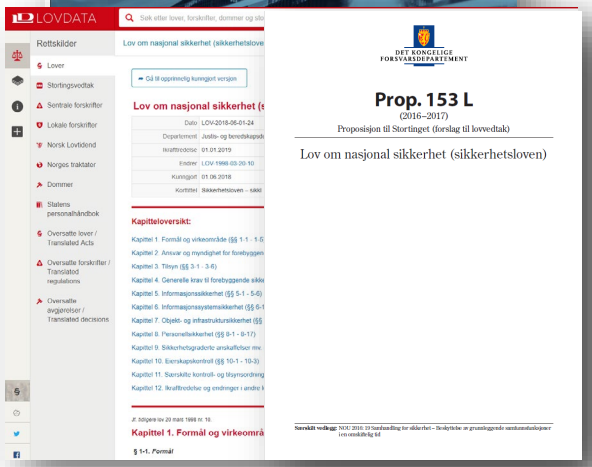
Til 3: Ulike regelverk – samme 5 "grunnkrav"



KVALE

Kilde: Odd Kleiva, DnB

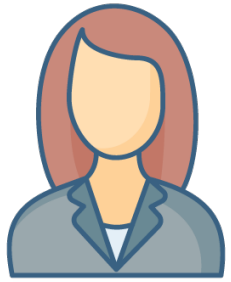
Til 3: Den grunnleggende utfordringen: oppfylle *funksjonelle minimumskrav* (som viser til rettslig standard)

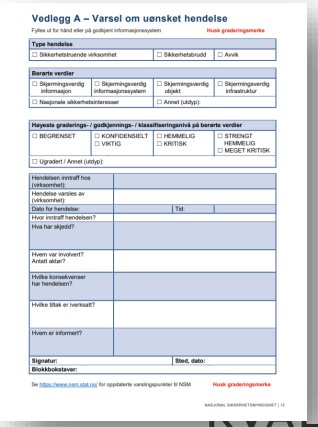


HANDLINGS-NORM

"forsvarlig sikkerhet"

Microsoft Active Directory





2. Hva er NIS2?

NIS2 på 1-2-3

1. **Hva?** *Oppdatering* av felles europeisk rammeverk for cybersikkerhet i nettverks- og informasjonssystem
2. **Når?** Frist 18. oktober 2024 for å gjennomføre direktiv (EU) 2022/2555
3. **Hvordan?** Direktiv som erstatter NIS (direktiv (EU) 2016/1148), utvidet virkeområde og strengere krav

("NIS" = Network and Information Security)

NIS2 under lupen

- **Minimumsharmonisering** (art. 5), nasjonal gjennomføring, strenger nasjonale krav hvis "consistent", felles virkeområde
- **"All hazards approach"** (art. 21), beskytte mot både trusselaktører og hendelser
- **Målsetting** (art. 1), motstandsdyktig infrastruktur - cybersikkerhet

(1) ‘cybersecurity’ means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

Forordning (EU) 2019/881 artikkel 2 (1) – Cybersecurity Act

NIS2 under lupen (forts.)

- **46** artikler, **144** fortalepunkt
- **Målgruppe:** både medlemsland (lovgiver og tilsyn) og offentlig/privat virksomheter
- Grunnleggende skille mellom **"essential entities"** og **"important entities",** betydning for:
  - Hvilke sektorer
  - Nivå på tilsyn/kontroll
  - Sanksjoner

KVALE

Når kommer NIS2 til Norge?

November 2022 – Vedtatt

Januar 2023 - I kraft

Oktober 2024 – Gjennomføring

2022

2023

2024

2025

Desember 2023 – NIS1 vedtatt

KVALE

Skriftlig spørsmål fra Linda Hofstad Helleland (H) til justis- og beredskapsministeren

Dokument nr. 15:588 (2023-2024)

Innlevert: 01.12.2023

Sendt: 04.12.2023

Besvart: 08.12.2023 av justis- og beredskapsminister Emilie Mehl

"Departementet har gitt DSB og NSM et oppdrag om å utarbeide forslag til hvordan NIS2-direktivet og CER-direktivet kan gjennomføres i norsk rett med frist våren 2024."

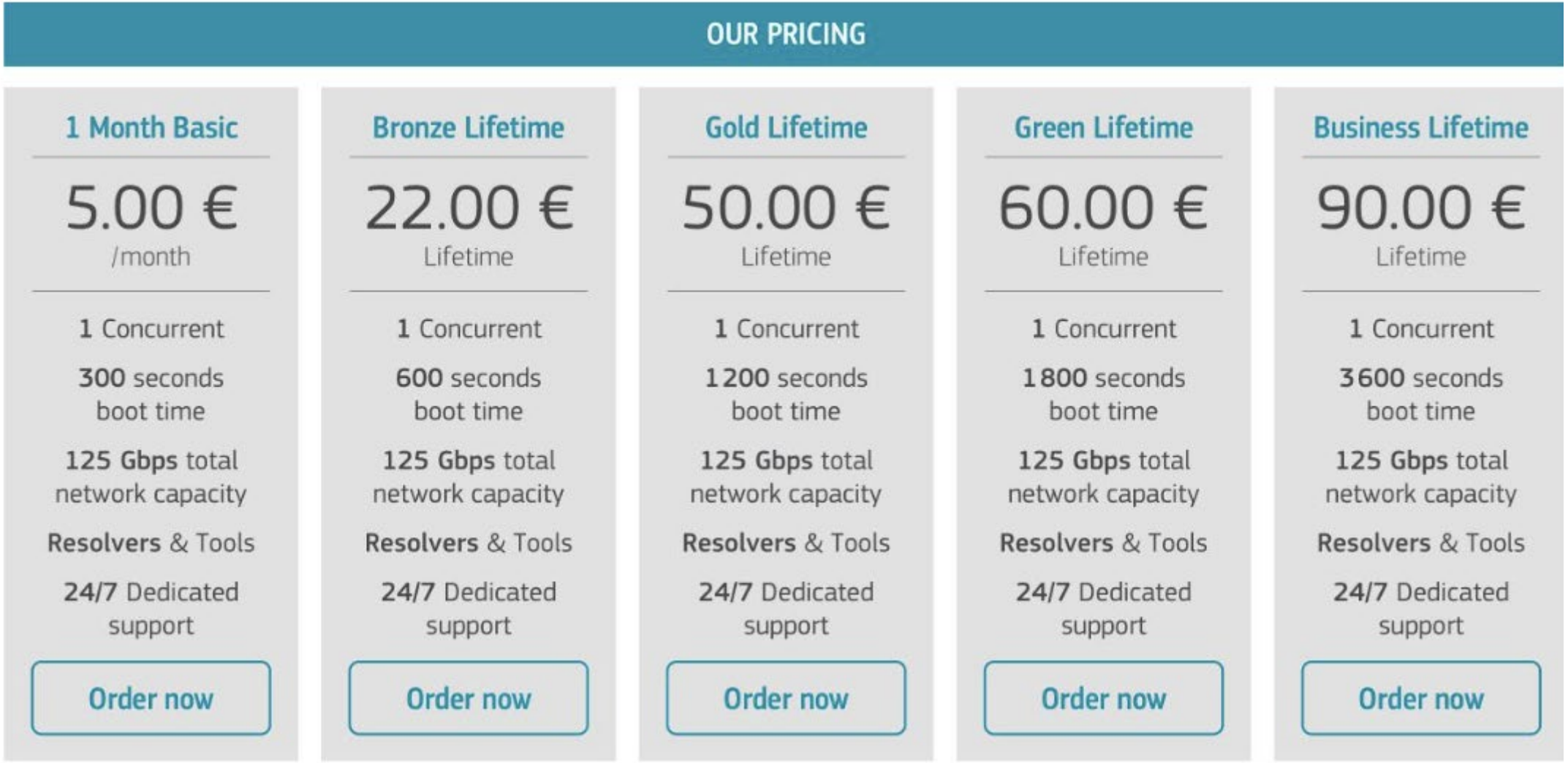
Spørsmål

Linda Hofstad Helleland (H): NIS2-direktivet må gjennomføres i EU innen 24. oktober 2024, mens det fortsatt er usikkert om når og hvordan direktivet eventuelt blir en del av norsk rett.

Vil regjeringen foreta seg noe for å sikre raskere tilpassing av norsk lov for å tilfredsstille kravene i NIS2-direktivet?

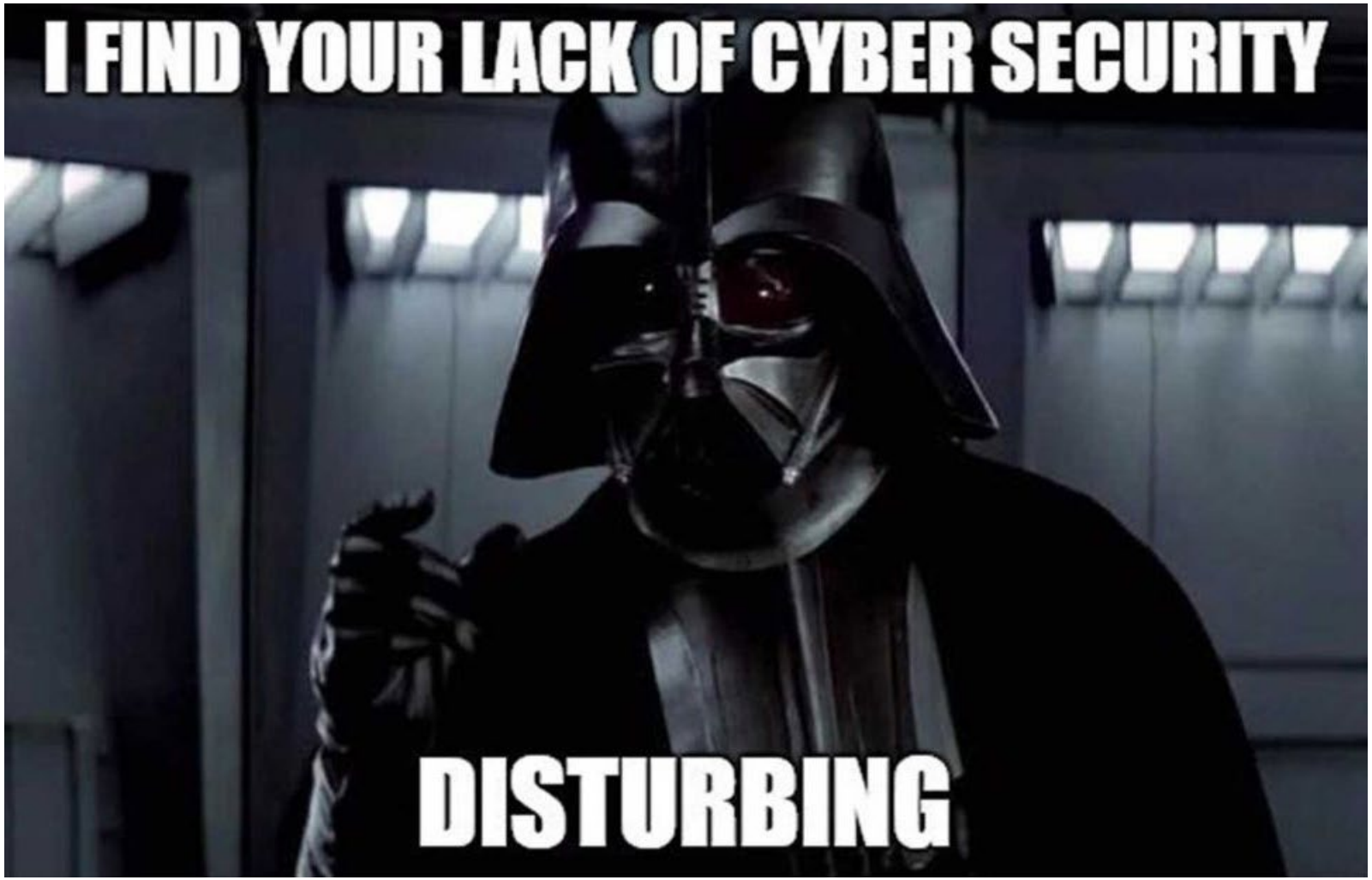
ALE

Hvorfor NIS2?



KVALE

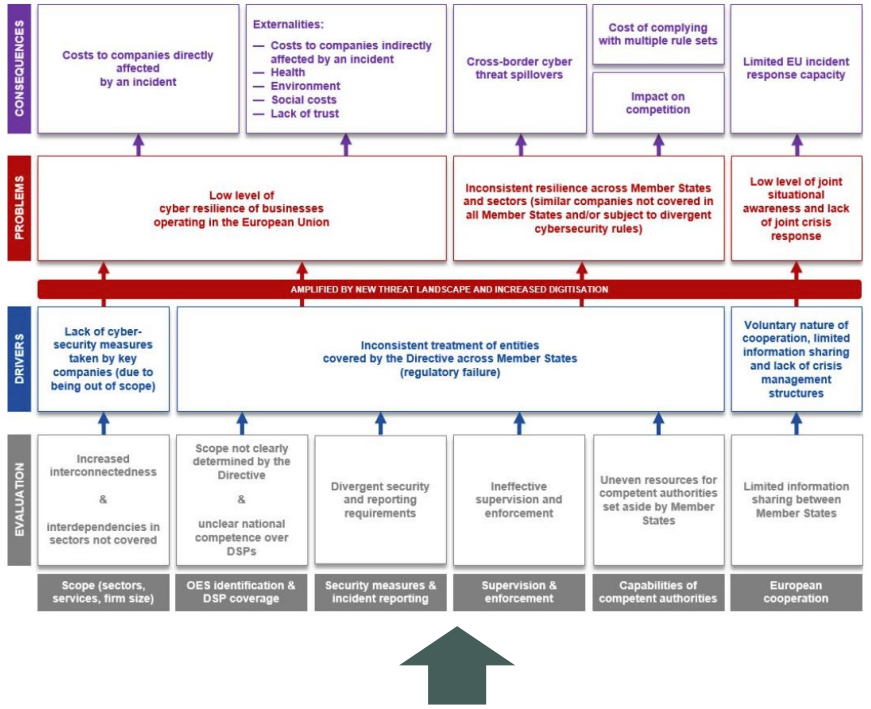
Hvorfor NIS2? (forts.)



KVALE

Hvorfor NIS2 (forts.)?

Lav motstandsdyktighet mot cyberhendelser i hele EU

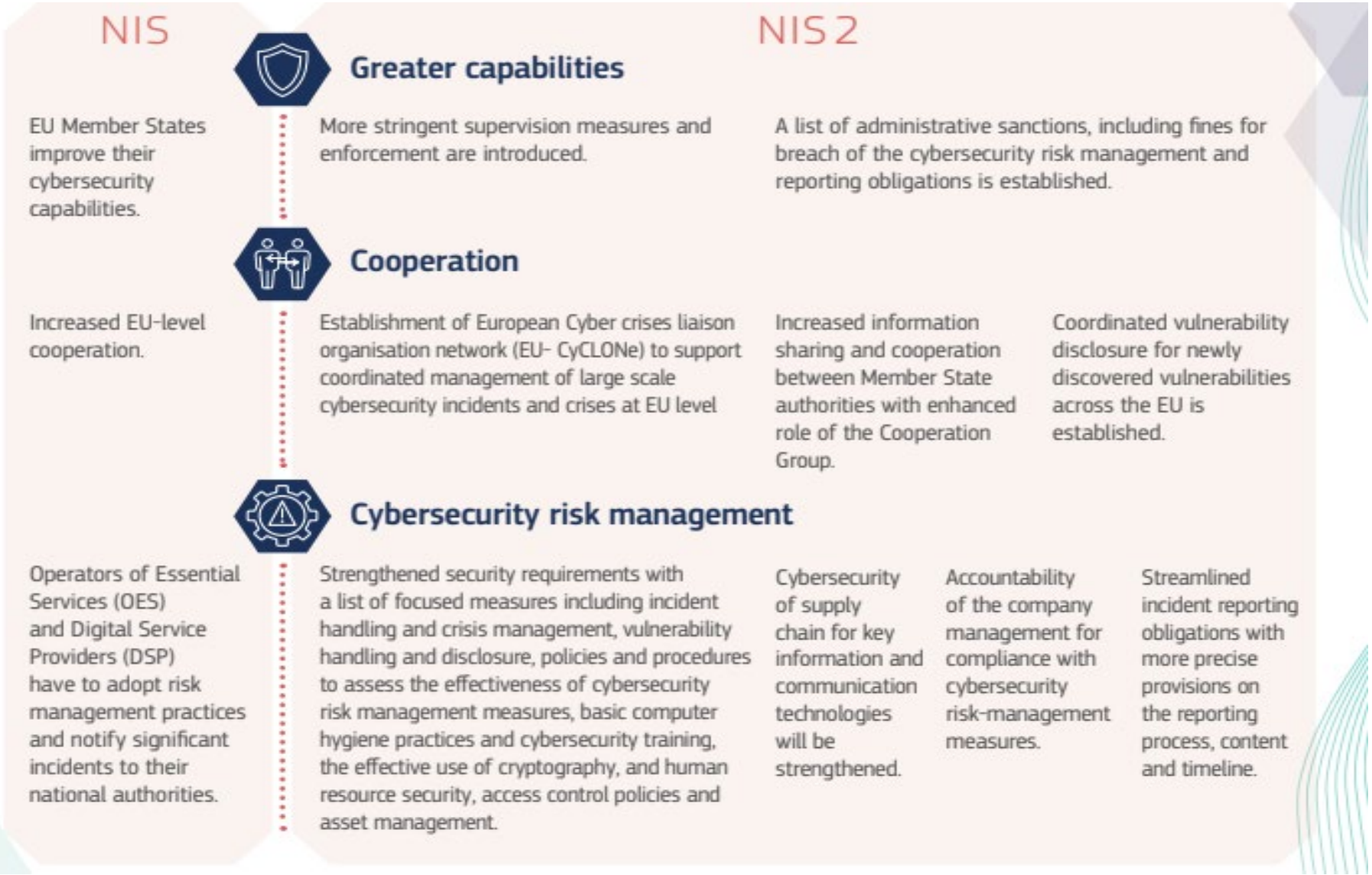


Ikke felles situasjonsforståelse eller krisehåndtering i EU

Fragmentert motstandsdyktighet i EU (manglende harmonisering)

KVALE

Hva er forskjellen på NIS og NIS2? – "Reboot"



STØRRE "VERKTØYKASSE"

STRENGERE KRAV TIL HARMONISERING OG SAMARBEID I EU/EØS

STRENGERE SIKKERHETSKRAV TIL OFFENTLIGE OG PRIVATE AKTØRER

KVALE

Hvorfor bør virksomheter ha NIS2 på radaren?

Fordi NIS2:

- ..utvider virkeområdet betraktelig
- ..stiller nye krav om varsling med korte frister
- ..pålegger en rekke nye minstekrav til sikkerhet basert på "all hazards approach"
- ...stiller "nye" minimumskrav til blant annet verdikjedesikkerhet og personellsikkerhet
- styreansvar og bøter på inntil 2 % av omsetning

Hvordan er NIS2 bygget opp?

- Chapter I: General provisions — Art. 2, 3, 4 og 6
- Chapter II: Co-ordinated cybersecurity frameworks
- Chapter III: Cooperation at Union and international level
- Chapter IV: Risk-management measures and reporting — Art. 20, 21 og 23
- Chapter V: Jurisdiction and registration — Art. 26
- Chapter VI : Information sharing
- Chapter VII: Supervision and enforcement — Art. 32, 33 og 34
- Chapter VIII: Delegated and implementing acts
- Chapter IX: Final provisions
- Annex I and II

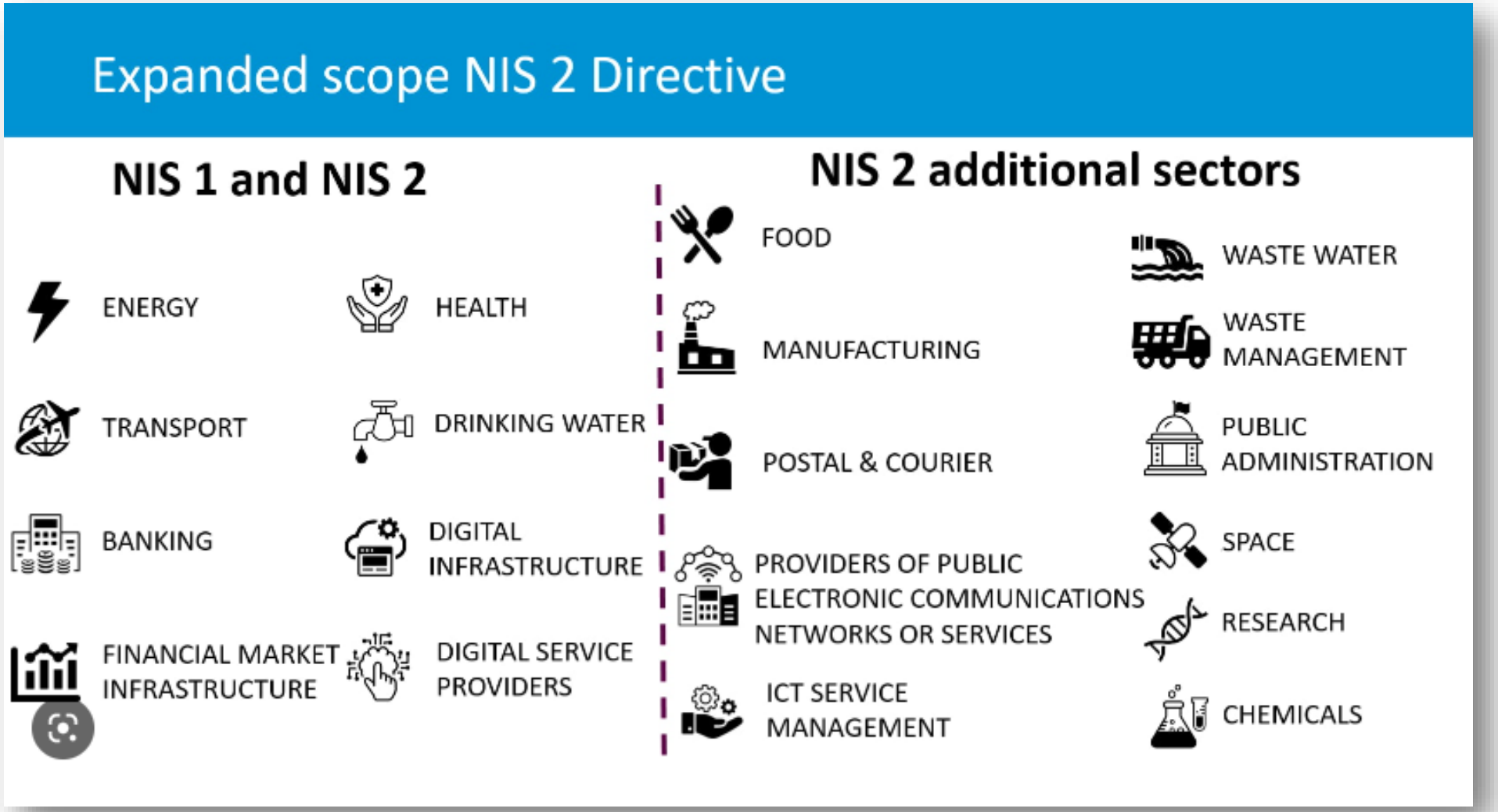
KVALE

3. Når gjelder NIS2, for hvem og hvor?

Når er virksomheten underlagt NIS2?

KVALE

Til 1) Hvilke sektorer gjelder NIS2 for?



KVALE

Til 2) Hvor stor må virksomheten være?

	ESSENTIAL ENTITIES (EE)	IMPORTANT ENTITIES (IE)
Terskelverdi, art. 2 nr. 1 og 3, ref. 2003/361 EC	**Terskelverdi:** *Generelt* +250 ansatte, EUR + 50 millioner i årlige omsetning eller balanse på EUR +43 millioner – ANNEX I	**Terskelverdi:** *Generelt* +50 ansatte, EUR + 10 millioner i årlige omsetning eller balanse på EUR +13 millioner – ANNEX II
Sektor spesifisert i vedlegg I og II	• Energi • Transport • Helse • Finans • Offentlig forvaltning (statlig, regionalt) • Romfart • Drikkevann og kloakk • Digital infrastruktur (inkl. TLD og DNS)	• Post- og kurertjenester • Avfallshåndtering • Bestemte typer produksjon • Mat • Kjemikalier • Forskning • Digital infrastruktur • Digitale tilbydere (OTT)

Til 3) Hvor i verden gjelder NIS2?

Art. 26 nr. 1: "[...] to fall under the jurisdiction of the Member State in which they are established, except in the case of:."

(113)" Entities falling within the scope of this Directive should be considered to fall under the jurisdiction of the Member State in which they are established. However, providers of public electronic communications networks or [...] should be considered to fall under the jurisdiction of the Member State in which they provide their services."

KVALE

4 a) Hvilke konsekvenser får NIS2 for privat og offentlig virksomhet?

Hvor finner du de operative kravene?

- Chapter I: General provisions
- Chapter II: Co-ordinated cybersecurity frameworks
- Chapter III: Cooperation at Union and international level
- Chapter IV: Risk-management measures and reporting — Art. 20, 21 og 23
- Chapter V: Jurisdiction and registration
- Chapter VI : Information sharing
- Chapter VII: Supervision and enforcement
- Chapter VIII: Delegated and implementing acts
- Chapter IX: Final provisions
- Annex I and II

KVALE

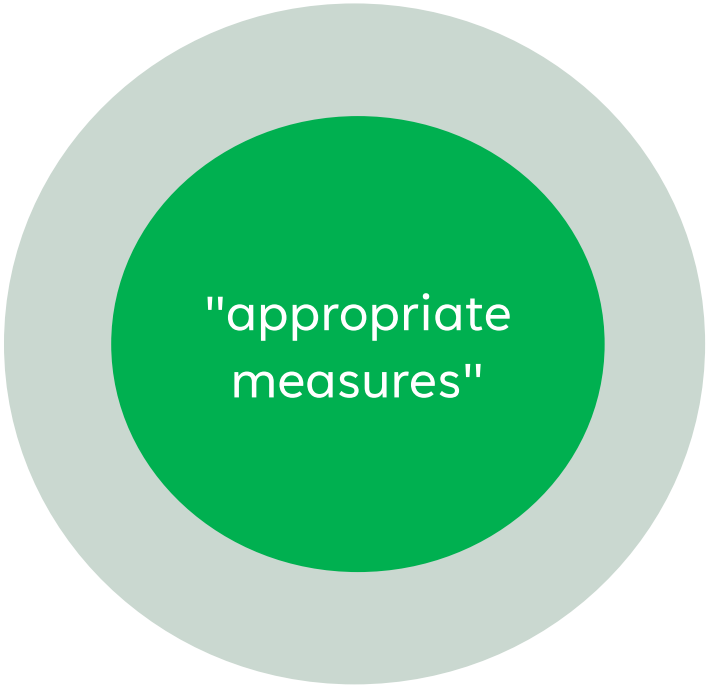
Hva må du vite om de de operative kravene?

- **Art. 20:** Styreansvar ("liability") for virksomhetens brudd på art. 21 (samt krav til oppæring)
- **Art. 21:** De operative minimumskravene til cybersikkerhet - i utgangspunktet de samme for IE og EE
- **Art. 23:** Omfattende varslingskrav for IE og EE med frister ved "vesentlige hendelser" - aktivitetsplikt for myndighet(er) som mottar varsel

KVALE

Hvilke sikkerhetskrav stiller art. 21?

Handlingsnorm (nr. 1)



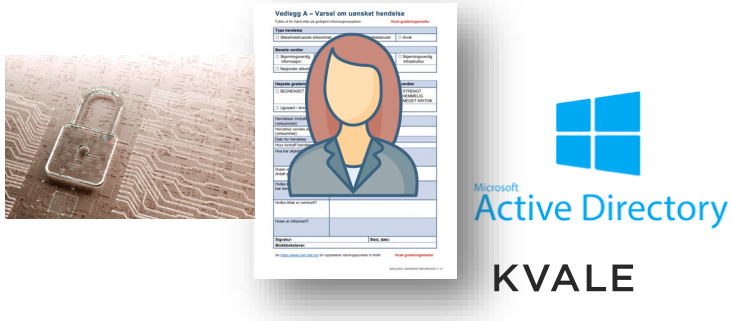
- "manage the risk"
- "prevent or minimise impact"

Rettslig standard (nr. 1)

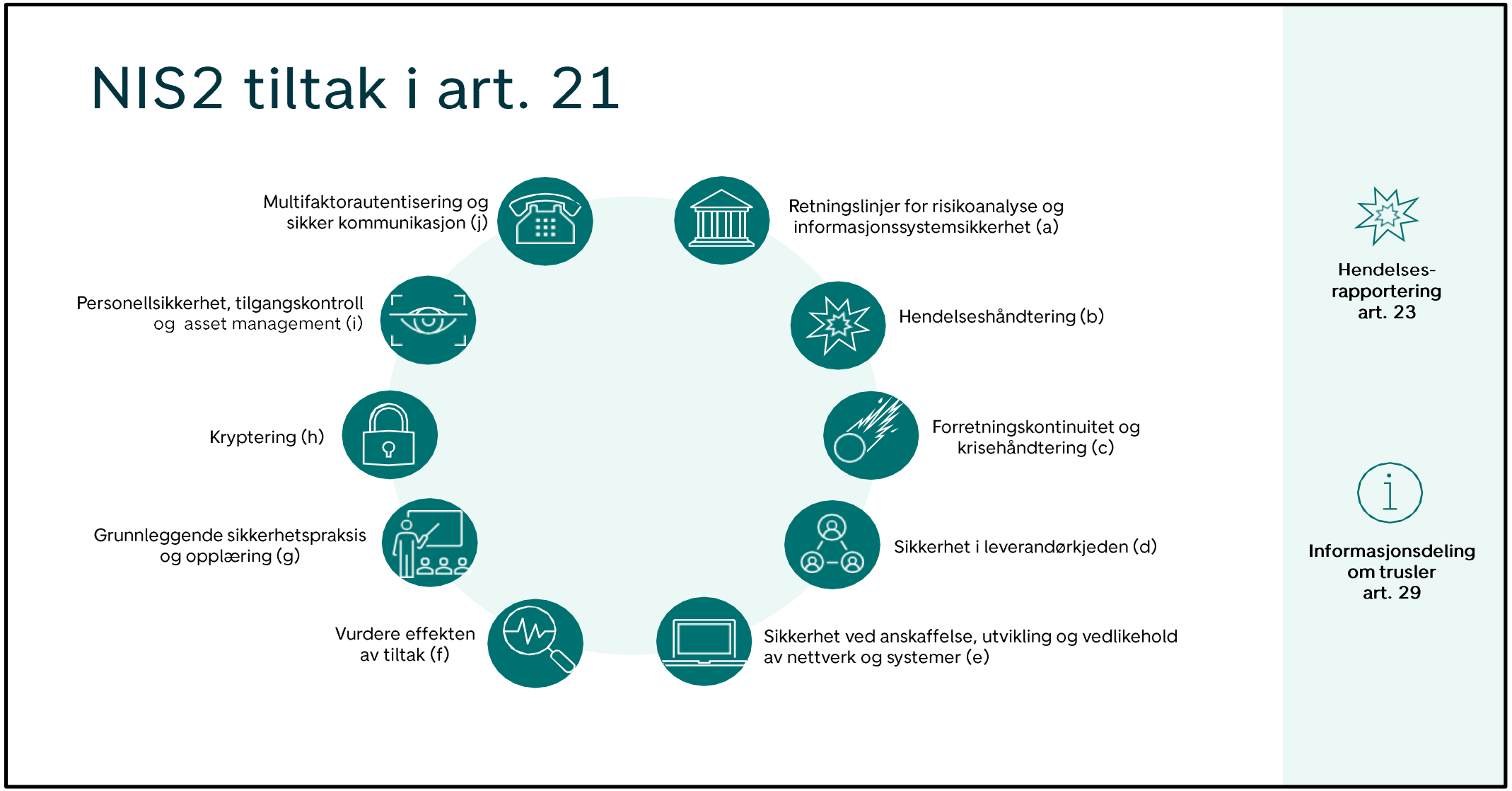
- "State of the art"
- "Standards"
- "Cost of implementation"
- "Level of security appropriate to the risk
- Entity´s exposure to risk, size, likelihood and severity
- "Social and economic impact"

Minimumskrav til tiltak (nr. 2)

- "All hazards"
- Beskytte logiske og fysiske verdier
- 10 kumulative krav som er listet opp i (a) til (j)



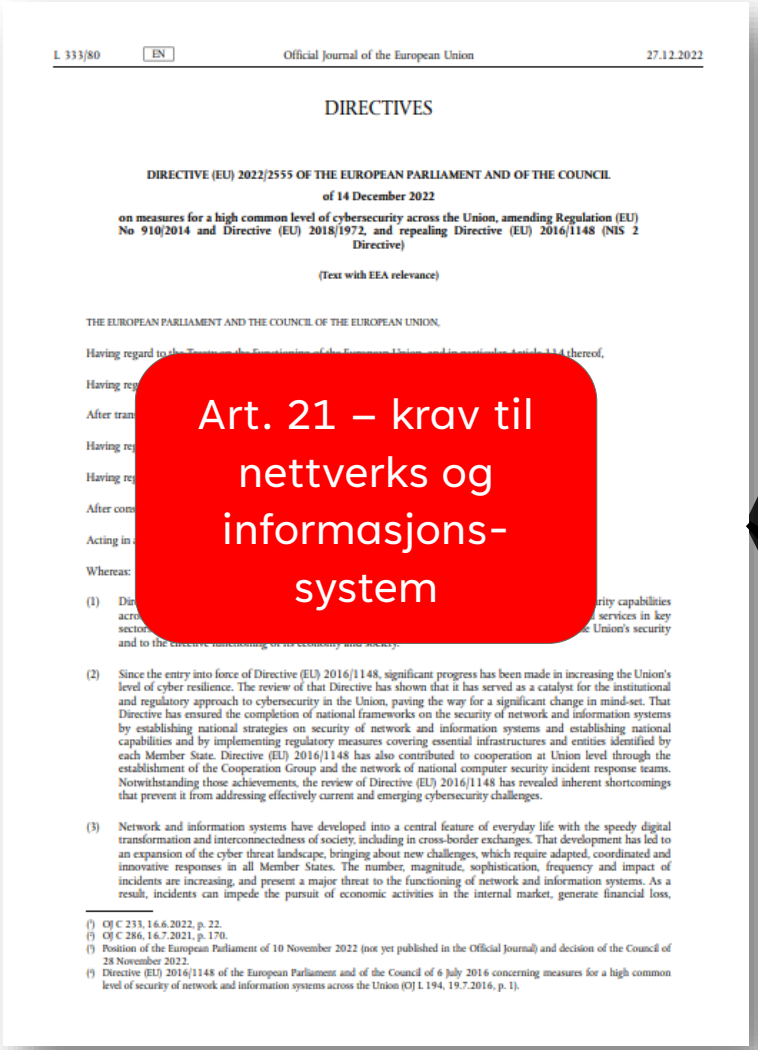
"Smørbrødlisten" i art. 21 nr. 2



KVALE

Kilde: Odd Kleiva, DnB

Hva blir mest krevende?



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

After consulting the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and of the Council (4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

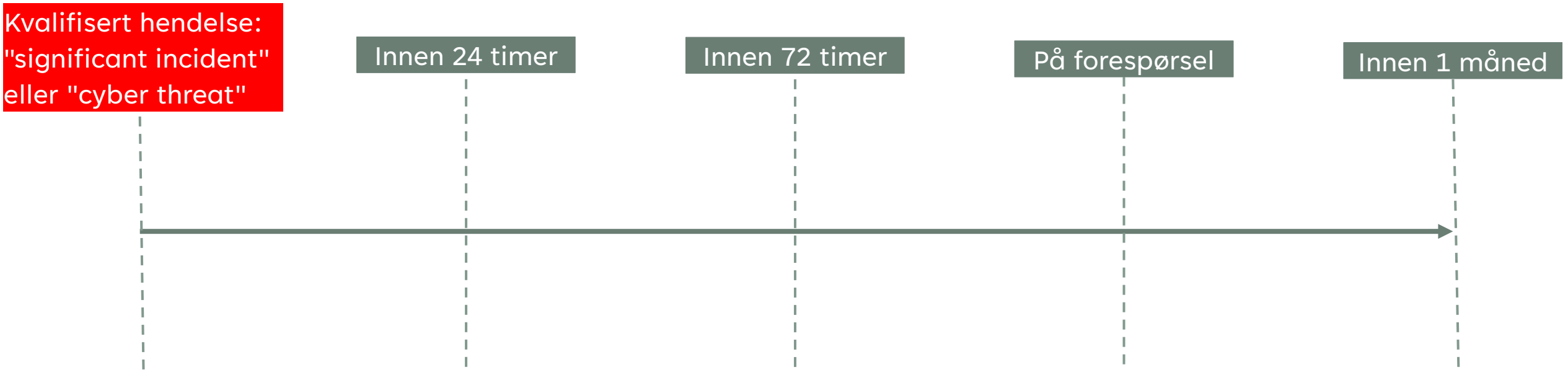
(1) OJ C 233, 16.6.2022, p. 22.
(2) OJ C 286, 16.7.2021, p. 170.
(3) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.
(4) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

Art. 21 – krav til nettverks og informasjons-system

- #1 Risikovurdering og internkontroll
- #2 Hendelseshåndtering
- #3 Beredskapsplanlegging og krisehåndtering
- #4 Verdikjedesikkerhet
- #5 Informasjonssystemsikkerhet (anskaffelse, utvikling)
- #6 Rutiner for test og revisjon
- #7 Cyberhygiene og opplæring
- #8 Rutiner for kryptografi og kryptering
- #9 Personellsikkerhet og tilgangsstyring
- #10 Multifaktorautentisering mv.

VALE

Hvilke krav stiller NIS2 til varsling? Art. 23



+ Varsle berørte mottakere av tjenester (nr. 2), "without undue delay"
+ Aktivitetsplikt for mottaker (nr. 5), "guidance and operational advice"
+ Varsle offentligheten (nr. 7), "after consulting the entity concerned"

KVALE

Hvilke krav stiller NIS2 til dokumentasjon?

- Ikke et generelt krav om "ansvarlighet" (GDPR art. 5 nr. 2) eller dokumentasjon (sikkerhetsloven § 4-4)
- Direkte krav i art. 21 nr. 2 (a), (f), (h) og (i).
- Indirekte krav for øvrige alternativer i art. 21
- Avgjørende for å "bevise" etterlevelse ved tilsyn og kontroll (det som ikke er skrevet ned, har ikke skjedd)

4 b) Hvilke konsekvenser får NIS2 for lovgiver og tilsynsmyndighet?

NIS2 vil stille krav til lovgiver og myndigheter på alle trinn

1. Vedtar/organiserer sikkerhetsregulering → 2. Veileder/ informerer/ støtter → 3. Forvalter/ fører tilsyn/ håndhever

Justis- og beredskapsdepartementet

Kommunal- og distriktsdepartementet

Eks. art. 4,5, 7, 9 og 21

DET KONGELEGE JUSTIS- OG BEREDSKAPSDEPARTEMENT

NASJONAL SIKKERHETSMYNDIGHET

Nasjonal kommunikasjons-myndighet

NVE

Eks. art. 21, 23 og 29

PST POLITIETS SIKKERHETSTJENESTE

POLITIET

SIVIL KLARERINGSMYNDIGHET

Datatilsynet

Nasjonal kommunikasjons-myndighet

NVE

Eks. art. 31, 32 og 33

Eksempel på konkrete krav

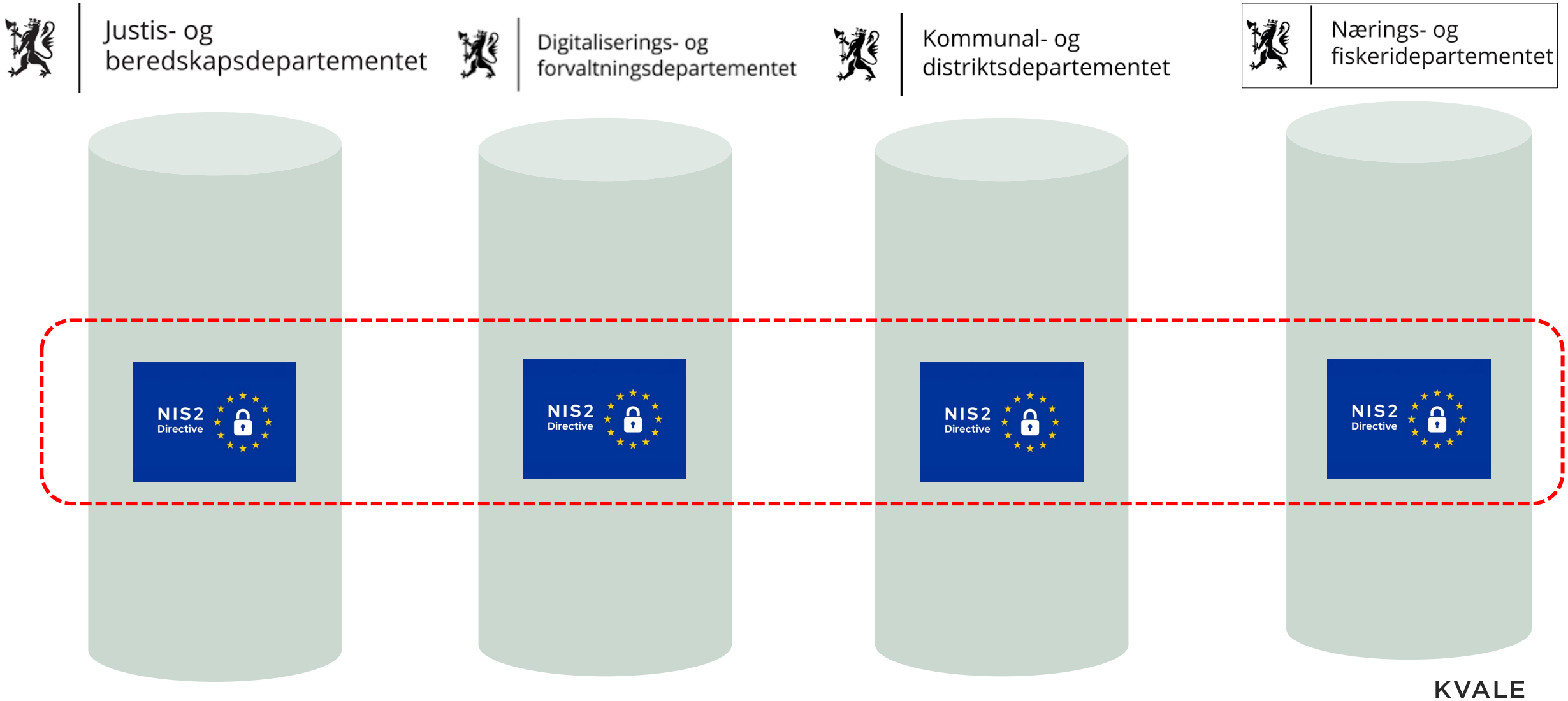
Til "lovgiver"

- Gjennomføre NIS2 i nasjonal rett innen fristen (minimumskrav)
- Teste andre regelverk mot NIS2 (art. 4)
- Sørge for at tilsynsmyndigheter, CSIRT og SPOC samarbeider med hverandre og andre myndigheter (politimyndigheter, personvern, ekom osv.)
- Utpeke eller etablere én eller flere kompetente tilsynsmyndigheter for cybersikkerhet, (art. 8)
- Utpeke eller etablere én eller flere Computer security incident response team (CSIRT) (art. 10 og 11, 12)

Til "tilsyn"

- Etablere en nasjonal cybersikkerhetsstrategi på nasjonalt nivå (plikt i punkt 1, minimumskrav i punkt 2, notifiseringsplikt i punkt 3), artikkel 7
- Bistå ved varsling om sikkerhetshendelser og publisere veiledning om terskelverdi, art. 23
- Etablere tekniske løsninger for å varsle, art. 23
- Etablere frivillig informasjonsdeling mellom regulerte virksomheter, art. 29

NIS2 vil utfordre "sektorprinsippet", i alle fall for kritisk infrastruktur



KVALE

Myndighetens verktøykasse blir større

Overtredelsesgebyr
Inntil 2% / EUR 50 mill.
eller 1,4 % / EUR 10 mill.

Rettepålegg

Advarsler

Informasjonsplikt
Overfor berørte

Informasjonsplikt
Overfor allmennheten
om overtredelser

(Rettssikkerhetsgarantiene i art. 32 nr. 7 og 8 dekker "hele verktøykassen")

Målrettet revisjon
Foretaket dekker
kostnaden

Dokumentasjon
På gjennomførte tiltak

Informasjonsplikt
Overfor allmennheten
om overtredelser

"Forvalter"
Til å overvåke
compliance i en periode

Suspensjon
Av tillatelse eller forbud
for fysisk person

5. Råd og tips

Egne erfaringer

- Sikkerhetsregulering = jus, noe få sikkerhetseksperter er klar over
- Alle vet fasiten etter en hendelse, få ønsker å veilede om den i forkant
- På sikkerhetsområdet er myndighetene (i vid forstand) den store tidsoptimisten
- Felles forståelse av handlingsnormen en forutsetning for å etterleve funksjonelle krav
- TTT

Råd og tips helt på tampen

- Kom i gang nå - det er INGEN grunn til å vente (og kommer til å få dårlig tid)!
- Finn ut om NIS2 treffer deg!
- Konsentrerer deg om de "sikre" kravene.
- Bruk et etablerte rammeverk og/eller anerkjente standarder (NSM, NIST, ISO osv.)
- Ta eierskap til hvordan din virksomhet skal oppfylle kravene
- Gjør noe – heller enn ingenting, du kommer langt med et ærlig forsøk

6. Spørsmål?

Snurr debatt!

- Når kommer NIS2 til Norge?
- Hvilke konsekvenser får NIS2 for norsk sektorregulering av sikkerhet?
- Vil NIS2 påvirke norsk tilsynspraksis?
- Hva blir det største utfordringen når det gjelder å etterleve NIS2?

Jens Christian Gjesti

Head of Tech & IP / Partner

jcg@kvale.no

90 20 20 72

KVALE

Om Kvale

- Siden oppstarten i 1988 har vi bistått nasjonalt og internasjonalt næringsliv. Vi er over 110 advokater basert i Oslo, Ålesund og Tromsø og er et ledende norsk forretningsadvokatfirma.
- Våre rangeringer i nasjonale og internasjonale rankinger bekrefter vår ledende posisjon i markedet.
- Vi bistår norske og internasjonale klienter, enten det er store selskap eller mindre virksomheter. I tillegg gir vi bistand til offentlige myndigheter og organisasjoner.
- Vi setter alltid det best kvalifiserte teamet for å bidra til kundens utvikling. Kvale er et true partnership, hvor alle partnerne kompenseres likt. På denne måten fremmer vi samarbeid og kunnskapsdeling og legger til rette for best mulig rådgivning og verdiskapning for kundene våre.
- Vi kombinerer en sterk **prestasjonskultur** med en sterk **samarbeidskultur** for å skape de beste resultatene for kundene våre. Vi skaper muligheter og kompetanseoverføring gjennom oppdragsgjennomføringen.