FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DORA

4. mars 2025

Tema

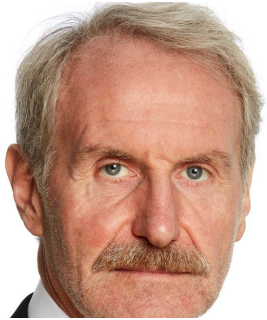
10:00	Kort om konserntematikk og samhandlingsmuligheter	Olav
10:20	Rapportering av hendelser	Åshild og Cecilie
11:30	Register over IKT-tjenesteavtaler (RoI, Register of Information)	Arild

Foredragsholderne

Cecilie Holth

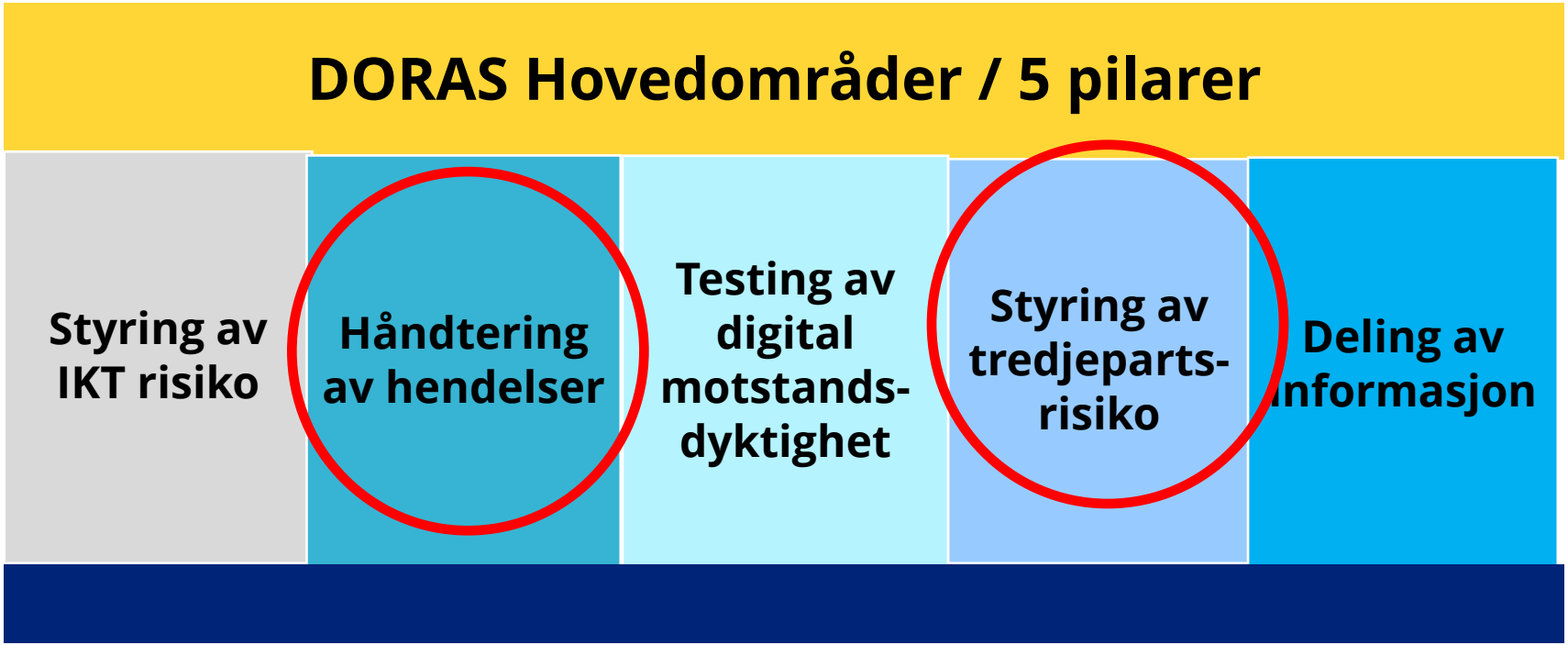
Åshild Johnsen

Arild Tømmerås



Olav Johannessen

DORA HOVEDOMRÅDER



Mottatte spørsmål

1. Vil det fra Finanstilsynets side komme tydelig og presis veiledning for hva man skal rapportere på?

   Vi tenker da både på format for rapportering, hvilke opplysninger man skal ha med, og detaljnivået på de ulike elementene?

Kort om konserntematikk og samhandlingsmuligheter

Konserntematikk

- **«Group» definert i DORA art. 3(26), videre henvisning til Direktiv 2013/34/EU art. 2(11):**

  «group» means a parent undertaking and all its subsidiary undertakings

- **Forstås som «konsern» - ikke samarbeidende grupper/allianser**

- **Konserntematikk aktuelt under flere av DORAs hovedområder**

Konserntematikk

- Adgang til å ha en helhetlig strategi for bruk av flere leverandører på gruppenivå (art 6 nr. 9)
- Finansforetak kan utkontraktere compliancefunksjon, forutsatt at det er tillatt i sektorregelverket (art. 6 nr. 10)
- Adgang til at leverandør rapporterer hendelser på foretakets vegne, forutsatt at det er tillatt i sektorregelverket (art. 19 nr. 5)
- Vurdere risiko på gruppenivå ved inngåelse av IKT-tjenesteavtaler (art. 28 nr.1 (b) (ii))
- IKT-tjenesteleverandører i konsern kan ikke pekes ut som gjenstand for oversight (art. 31 nr. 8 (iii))
- TLPT-testing for konsern med grenseoverskridende aktiviteter (fortale 57)
- Det er krav til at register over IKT-tjenesteavtaler skal foreligge på foretaksnivå, subkonsolidert nivå og konsolidert nivå (art. 28 nr. 3)
    - Registre over IKT-tjenesteavtaler som vedlikeholds og oppdateres på subkonsolidert og konsolidert nivå skal inkludere alle foretak som er del av konsernet (ITS 2024/2956 art. 6 (2))

Samhandlingsmuligheter

- **Samlet rapportering av hendelser**
- **Vil bli vurdert mht. melding om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner**
  - «De finansielle enhetene skal i god tid underrette den vedkommende myndigheten om enhver planlagt kontraktsregulert ordning om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, samt når en funksjon er blitt kritisk eller viktig.»

Rapportering av hendelser

Hva vi skal snakke om:

- Hendelsesrapportering etter IKT-forskriften
- Hendelsesrapportering etter DORA
- Praktisk løsning for rapportering etter DORA
- Videreformidling av rapporter

Hendelsesrapportering etter IKT-forskriften

Rapportering etter IKT-forskriften

IKT-forskriften § 9 tredje ledd - Avviks- og endringshåndtering

Operasjonelle hendelser eller sikkerhetshendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data skal uten ugrunnet opphold rapporteres til Finanstilsynet. Rapporteringen skal normalt omfatte hendelser som foretaket selv kategoriserer til alvorlighetsgrad svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk.

Rapportering etter IKT-forskriften

- IKT-forskriften § 1 - virkeområde:

  Forskriften gjelder for:
  - Banker
  - Kredittforetak
  - Finansieringsforetak
  - Forsikringsforetak
  - Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond
  - Børser og autoriserte markedsplasser
  - Verdipapirforetak
  - Forvaltningsselskaper for verdipapirfond
  - Inkassoselskap
  - Eiendomsmeglerforetak
  - Betalingsforetak og opplysningsfullmektiger
  - E-pengeforetak
  - Systemer for betalingstjenester

- Eiendomsmeglerforetak omfattes ikke av krav til hendelsesrapportering, jf. § 9 (3)

Hendelsesrapportering etter DORA

Regler for hendelsesrapportering etter DORA

Nivå 1-regelverk

DORA kapittel III, art. 17-23

- Prosess for håndtering av IKT-relaterte hendelser
- Kriterier for klassifisering av hendelser og cybertrusler
- Krav knyttet til rapportering

Nivå 2-regelverk

RTS 2024/1772 om klassifisering og terskelverdier

RTS 2025/301 om innhold og tidsfrister for rapportering

ITS 2025/302 med utfyllende bestemmelser og skjemaer, maler og prosedyrer for rapportering

Rapportering av alvorlige IKT-relaterte hendelser

- Hvem skal rapportere?
- Hvilke hendelser skal rapporteres?
- Frister for rapportering
- Innhold i rapportene
- Annet

Hvem skal rapportere?

- Finansielle enheter som definert i art. DORA art. 2(1)(a)-(t):
  - kredittinstitusjoner
  - betalingsforetak
  - opplysningsfullmektige
  - e-pengeforetak
  - verdipapirforetak
  - tilbydere av tjenester knyttet til kryptoverdier
  - verdipapirsentraler
  - sentrale motparter
  - handelsplasser
  - transaksjonsregistre
  - forvaltere av alternative investeringsfond
  - forvaltningsselskaper
  - leverandører av datarapporteringstjenester
  - forsikrings- og gjenforsikringsforetak
  - forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikringsformidlere
  - pensjonsforetak
  - kredittvurderingsbyråer
  - administratorer av kritiske referanseverdier
  - tjenesteleverandører for folkefinansiering
  - verdipapiriseringsregistre

Hvem skal rapportere? (forts.)

- Noen foretak er unntatt fra reglene i DORA (art. 2(3))
- Flere foretakstyper kan bli underlagt rapporteringsplikt i forbindelse med innføring av DORA gjennom lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven
- Proporsjonalitetsprinsipp (art. 4(2))
  - Gjelder for regler om hendelsesrapportering
  - Regelverket stiller mer omfattende krav til noen foretakstyper enn andre

Hvilke hendelser skal rapporteres?

Rapporteringsplikt for "alvorlige" IKT-relaterte hendelser til Finanstilsynet (DORA art. 19(1))

Foretakene må vurdere hendelsen ut fra vilkår og vurderingsmomenter i nivå 1- og 2-regelverket for å avgjøre om hendelsen kan klassifiseres som "alvorlig"

Vurderingsmomenter ved klassifisering, DORA art. 18(1) og RTS 2024/1772 art. 1-7:

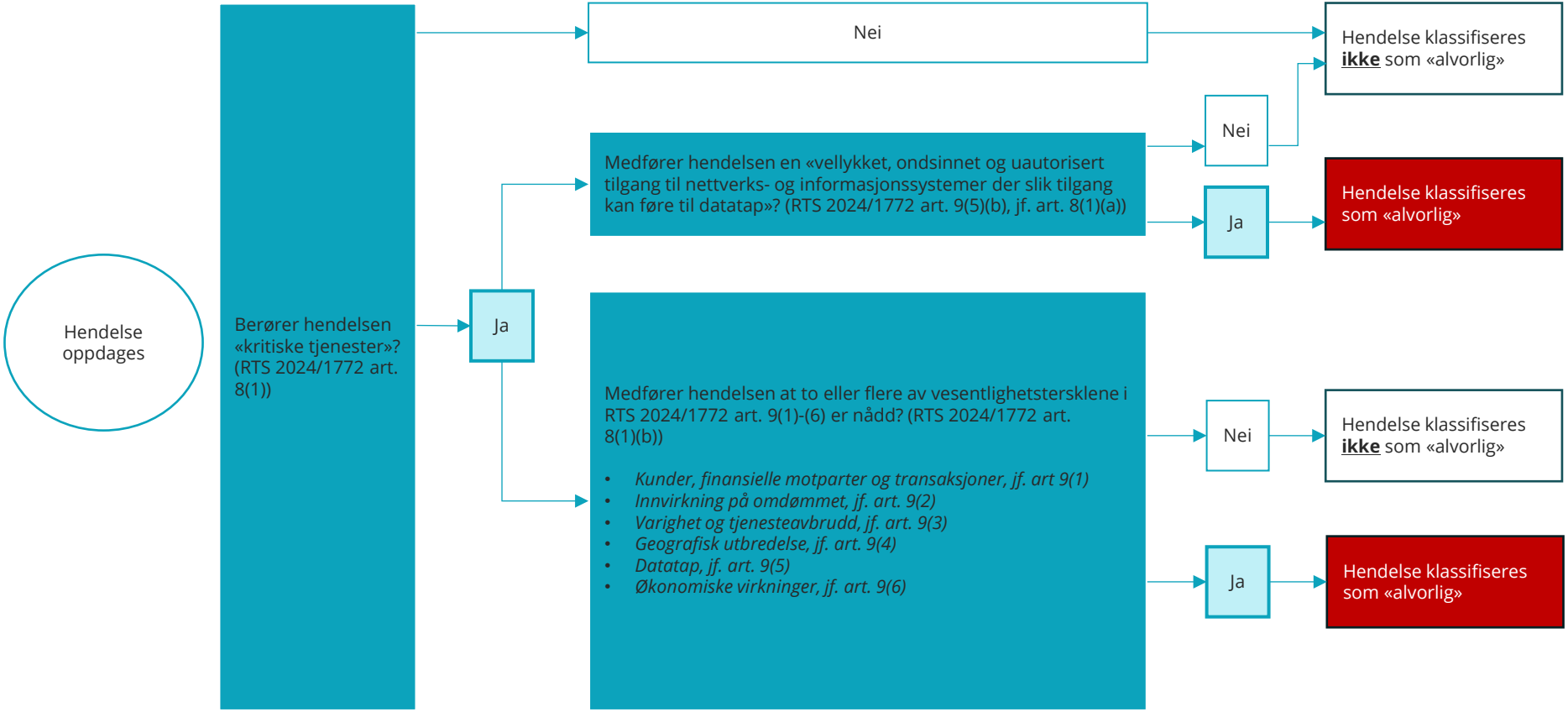
- Kunder, finansielle motparter og transaksjoner
- Innvirkning på omdømmet
- Varighet og tjenesteavbrudd
- Geografisk utbredelse
- Datatap
- De berørte tjenesters kritiske betydning
- Økonomiske virkninger

Hvilke hendelser skal rapporteres? (forts.)

Kriterier for "alvorlig" IKT-relatert hendelse (RTS 2024/1772 art. 8(1)):

1. Påvirker "kritiske tjenester" (art. 6);

2. Ett av følgende vilkår er oppfylt:
    i. enhver vellykket, ondsinnet og uautorisert tilgang til nettverks- og informasjonssystemer, hvor slik tilgang kan resultere i datatap (art. 9(5)(b), jf. art. 8(1)(a))
    ii. to eller flere av vesentlighetstersklene i art. 9(1)-(6) er nådd (jf. art. 8(1)(b))


Hendelse oppdages
Berører hendelsen «kritiske tjenester»? (RTS 2024/1772 art. 8(1))
Nei
Hendelse klassifiseres **ikke** som «alvorlig»
Ja
Medfører hendelsen en «vellykket, ondsinnet og uautorisert tilgang til nettverks- og informasjonssystemer der slik tilgang kan føre til datatap»? (RTS 2024/1772 art. 9(5)(b), jf. art. 8(1)(a))
Nei
Hendelse klassifiseres **ikke** som «alvorlig»
Ja
Hendelse klassifiseres som «alvorlig»
Medfører hendelsen at to eller flere av vesentlighetstersklene i RTS 2024/1772 art. 9(1)-(6) er nådd? (RTS 2024/1772 art. 8(1)(b))
• *Kunder, finansielle motparter og transaksjoner, jf. art 9(1)*
• *Innvirkning på omdømmet, jf. art. 9(2)*
• *Varighet og tjenesteavbrudd, jf. art. 9(3)*
• *Geografisk utbredelse, jf. art. 9(4)*
• *Datatap, jf. art. 9(5)*
• *Økonomiske virkninger, jf. art. 9(6)*
Nei
Hendelse klassifiseres **ikke** som «alvorlig»
Ja
Hendelse klassifiseres som «alvorlig»

Frister for rapportering

Innledende varsling

- **Så snart som mulig,** men innen 4 t fra klassifisering og senest innen 24 t fra foretaket oppdaget hendelsen (RTS 2025/301 art. 5(1)(a))

Statusrapport

- **Så snart som mulig** der status på opprinnelig hendelse har endret seg vesentlig eller håndteringen av den har endret seg basert på ny informasjon (DORA art. 19(4)(b))
- Når normale aktiviteter har blitt gjenopptatt (RTS 2025/301 art. 5(1)(b))
- Senest innen 72 t fra innledende varsling (RTS 2025/301 art. 5(1)(b))
- På forespørsel fra Finanstilsynet (DORA art. 19(4)(b))

Endelig rapport

- Senest innen én måned etter siste statusrapport (RTS 2025/301 art. 5(1)(c))

Innhold i rapportene

- Krav til standardisert form i tråd med krav i nivå 2-regelverk (ITS 2025/302 art. 1)
- Det stilles krav til hvilken type informasjon som skal være med i de ulike rapportene (RTS 2025/301 art. 1-4)
- Standardmalen for de ulike rapporttypene har både obligatoriske og betingede felt

Rapport	Antall obligatoriske felt	Antall betingede felt
Generell informasjon	10	6
Innledende rapport	7	3
Statusrapport	14	21
Endelig rapport	11	5
Totalt	**42**	**35**

Annet

Informasjon til berørte kunder
DORA art. 19(3)

- Påvirket kundenes økonomiske interesser
- Uten ugrunnet opphold
- Beskrive tiltakene som er gjort for å begrense skadevirkningene

Utkontraktering av rapporteringsforpliktelser
DORA art. 19(5) og ITS 2025/302 art. 6

- Kan utkontraktere til tredjepartsleverandør, men forblir ansvarlig
- Må meldes til Finanstilsynet

Aggregert rapportering
ITS 2025/302 art. 7

- Tredjepartsleverandører kan rapportere på vegne av flere etter visse vilkår
- Krav i DORA art. 19(5) og ITS 2025/302 art. 6 må være oppfylt
- Noen unntak, eks. handelsplasser og sentrale motparter

Annet (forts.)

Tilbakevendende hendelser

RTS 2024/1772 art. 8(2) og ITS 2025/302 art. 3

- Mindre og tilbakevendende hendelser kan samlet klassifiseres som "alvorlig"
- Informasjon til Finanstilsynet i aggregert format

Reklassifisering av hendelser

ITS 2025/302 art. 5

- Hendelse oppfylte aldri vilkår som «alvorlig» hendelse
- Meldes til Finanstilsynet

Frivillig rapportering av betydelige cybertrusler

▪Frivillig å rapportere «betydelige» cybertrusler (DORA art.19(2))

▪Kriterier for "betydelige" cybertrusler (RTS 2024/1772 art. 10)

1. cybertrusselen, om den materialiseres, kan **påvirke eller kan ha påvirket foretakets kritiske eller viktige funksjoner eller andre tredjeparter** basert på informasjon som er tilgjengelig for foretaket;
2. **høy sannsynlighet** for at cybertrusselen vil **materialisere seg** i den finansielle enheten eller andre finansielle enheter;
3. hvis cybertrusselen materialiseres, kan den oppfylle ett av **kriteriene i art. 10 (c)**

▪Krav til standardisert form i tråd med krav i nivå 2-regelverk (ITS 2025/302 art. 8)

▪Et cyberangrep som har skjedd skal rapporteres som en alvorlig IKT-relatert hendelse

Praktisk løsning for rapportering

Praktisk løsning for rapportering til Finanstilsynet

Standardformatet for rapportering er av de europeiske tilsynsmyndighetene definert i JSON og Excel

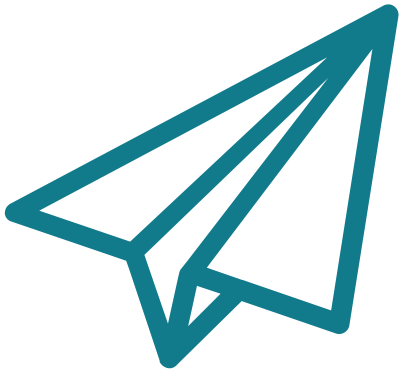
Excel-skjemaene kan lastes ned fra via denne lenken

Finanstilsynet utvikler et Altinn app-skjema i henhold til standardformatet. Informasjonen i webskjemaene vil bli konvertert til JSON før rapportene blir videresendt til De europeiske tilsynsmyndighetene

I spesielle tilfeller kan foretak rapportere på Excel-skjemaet som vedlegg til e-post og sende til hendelse@finanstilsynet.no

Oppfordring om å skrive på engelsk, men ikke et krav

Veileder om hendelsesrapportering vil publiseres på finanstilsynet.no



Videreformidling av rapporter

Videreformidling av rapporter

Finanstilsynet skal, uten ugrunnet opphold, videresende hendelsesrapporter til De europeiske tilsynsmyndighetene (EBA, ESMA eller EIOPA) (DORA art. 19(6)(a))

Finanstilsynet vil motta rapporter fra EBA, ESMA eller EIOPA for hendelser som er relevante for Norge (RTS 2024/1772 art. 11**).** Gjelder for hendelser som rammer norske filialer av utenlandske foretak

Norske filialer av utenlandske foretak oppfordres til å rapportere om hendelser direkte til Finanstilsynet frem til DORA trer i kraft i Norge

Spørsmål?

Register over IKT-tjenesteavtaler

(RoI - Register of Information)

Hva vi skal snakke om:

- Kort om hensikt
- Hvem skal ha register
- Når det skal være på plass
- Hva skal rapporteres

Hensikten med registeret

Styring av IKT-tredjepartsrisiko i foretaket

Forenkle tilsynsvirksomheten

Avdekke konsentrasjonsrisiko i  og 

Alle foretak omfattet av DORA skal ha et register!

Når må registeret være på plass?

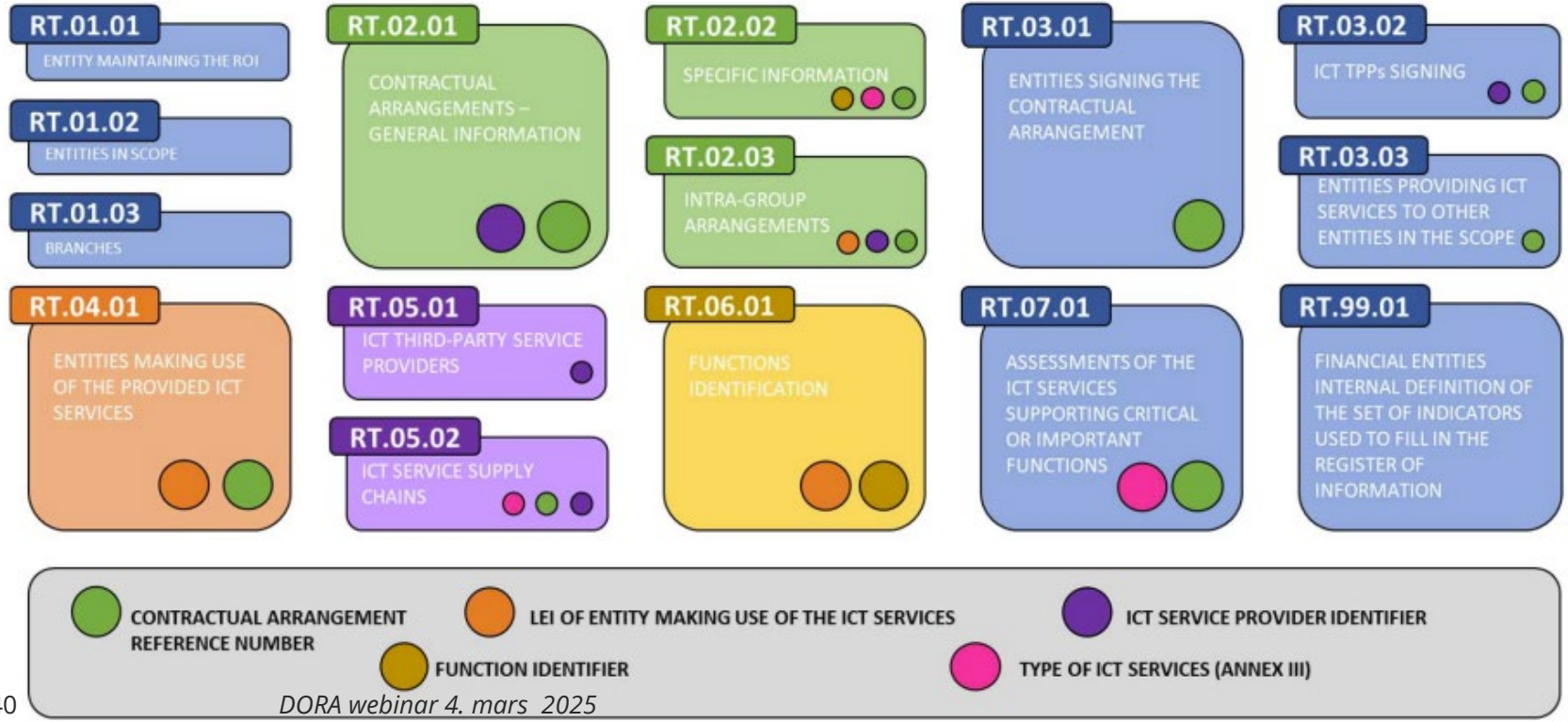
Når lov om
digital operasjonell
motstandsdyktighet
trer i kraft i Norge

Hvem skal rapportere?

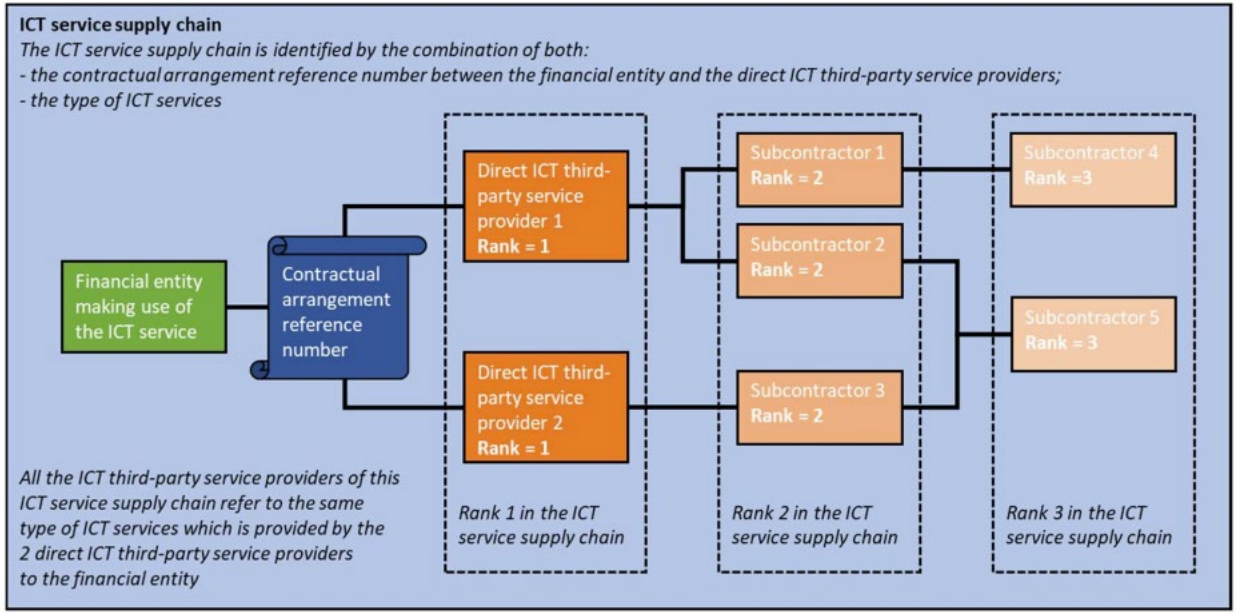
- Alle foretak som er underlagt DORA
- I konsern skal foretaket på høyeste nivå rapportere til hjemlandsyndigheten i EU/EØS.

Register i konsern

Hva registeret skal inneholde



Leverandørkjeder



Hva skal rapporteres?

Informasjon om alle kritiske eller viktige IKT-tjenesteavtaler for foregående år

NB! IKT-tjenesteavtaler ≠ utkontraktering

Maler ligger på siden til EBA

Rapporteringen

Når skal det rapporteres

Foretakene:

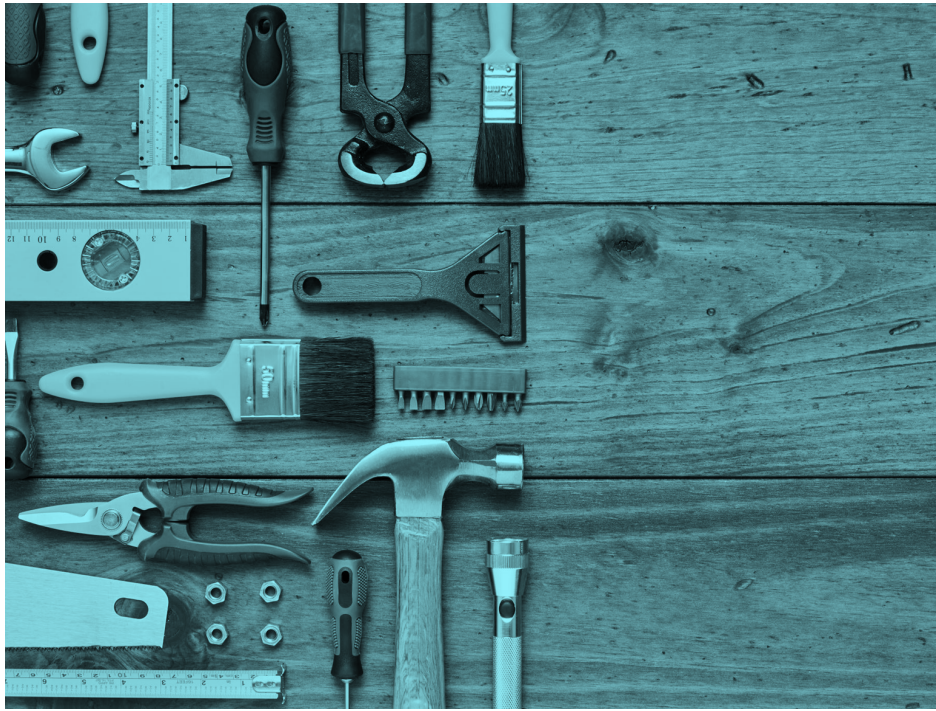
- ❑ Norske foretak skal ikke rapportere før DORA trer i kraft
- ❑ Årlig rapportering eller når Finanstilsynet ber om det
- ❑ Eksakt dato er ikke fastsatt

Finanstilsynets frist:

- ❑ Innen 31. mars 2026 til EBA.
- ❑ Register for foregående år

Hvordan skal det rapporteres (verktøy/format)

- Format: XBRL CSV- se XBRLs hjemmeside
- Antagelig lenke med autentisering via ALTINN



Hvordan forberede seg

- Vurder anskaffelse av verktøy for registerføring
- Følg med på informasjonssider på FT og EBA
- Gjennomgå alle kritiske og viktige tjenesteavtaler for IKT
- Samle leverandørdata iht. til maler – spesielt EUID og LEI-nummer
- Skaff LEI-nummer hvis foretaket ikke har det

Viktige lenker

ITS: (EU) 2024/2956

EBAs infromasjonsside for forberedelser for rapportering av RoI:
Preparations for reporting of DORA registers of information

ESA-enes FAQ: Frequently Asked Questions

Finanstilsynets side om ROI: Kommer

Sende inn spørsmål til oss: DORAQ&A@finanstilsynet.no

Finanstilsynets Q&A: Q&A DORA

Spørsmål?

Lenke til norsk uoff. oversettelse av DORA

https://lovdata.no/static/NLX3/32022r2554.pdf

FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY