FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Det forenklede rammeverket for IKT-risikostyring under DORA

Ida Kvernebo Mackenzie og Jarleif Lødøen

Avdeling for Risikoovervåkning og Makrotilsyn

Seksjon for tilsyn med IT og betalingstjenester

Oslo, 16. januar 2026

Innhold i presentasjonen

- Overordnet om rettslig plassering og proporsjonalitet
- Rammeverk for IKT-risikostyring under DORA
- Nærmere om det forenklede rammeverket for IKT-risikostyring

Rettslig plassering og proporsjonalitet

Finansforetaksloven

- Generelle krav til styring og kontroll

DORA-forordningen

- Spesielle krav til styring og kontroll for IKT-virksomheten

DORA-forordningen

Gjennomført i DORA-loven

Gjelder som norsk lov

Nivå 2-regelverk

Gjennomført i DORA-forskriften

Gjelder som norsk lov

Proporsjonalitet – DORA art. 4

Rammeverk for IKT-risikostyring under DORA

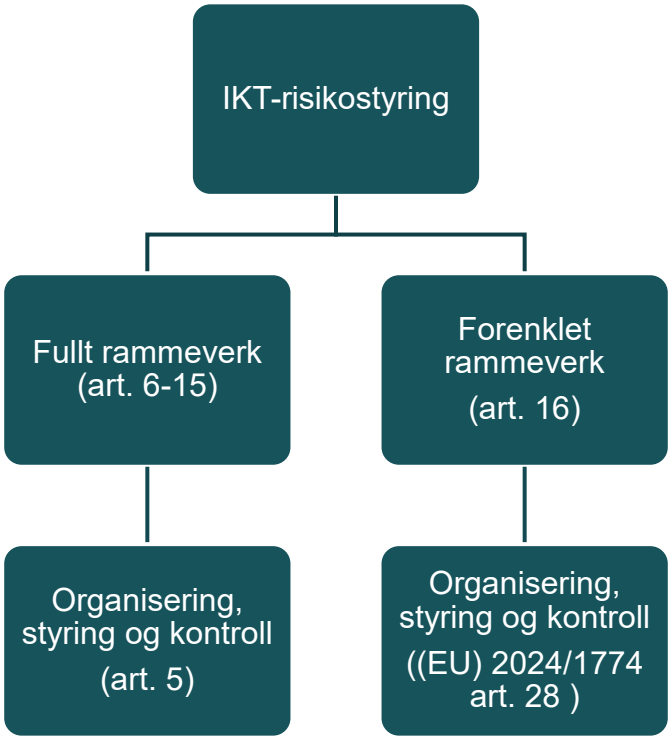
To rammeverk for IKT-risikostyring i DORA

Fullt rammeverk

Forenklet rammeverk

DORA – IKT-risikostyring:

Organisering, styring og kontroll



Foretakets størrelse avgjør ikke hvilket rammeverk foretaket skal etterleve!

Forenklet rammeverk

- Små verdipapirforetak uten innbyrdes forbindelse
- Betalingsforetak med begrenset tillatelse
- E-pengeforetak med begrenset virksomhet
- Små tjenestepensjonsforetak (se DORA art. 3 nr. 63)

Fullt rammeverk

- Øvrige foretak underlagt DORA

Nærmere om det forenklede rammeverket for IKT-risikostyring

DORA-Forordningen

Om DORA-loven for små foretak

Regelverket i Artikkel 16 – Link til DORA-Loven

- **DORAs målsetning med rammeverket for risikostyring:**
  - Høyt nivå av digital operasjonell robusthet i hele den finansielle sektoren i EU

- **DORAs mål med det forenklet rammeverket for IKT-risikostyring art. 16 i DORA-loven:**
  - Høy robusthet for foretakstypene som er omfattet av dette rammeverket. Hensikten er at de skal slippe de mest ressurskrevende delene av kapittel II (Art. 5–15) i DORA-forordningen, men likevel må opprettholde et minimum av forsvarlig IKT-risikostyring.

Intensjonen bak det forenklede rammeverket for IKT-risikostyring

Mål / Hensikt	Hvordan Art. 16 bidrar
Unngå uforholdsmessig byrde	Fjerner krav om bl.a. detaljert resilience-strategi, tre forsvarslinjer modell, årlig revisjon, egen krisehåndteringsfunksjon, obligatorisk strategi for flerleverandør osv.
Beholde grunnleggende beskyttelse	Selv de minste skal ha dokumentasjon, grunnleggende deteksjon, back-up/gjenoppretting og testing
Fremme proporsjonalitet i praksis	Klart signal om: jo mindre og mindre kompleks → jo enklere krav
Sikre et minimum av harmonisering	Kravene skal være tilnærmet like på tvers av EU-land
Legge til rette for tilsyn	Myndighetene kan fortsatt be om dokumentasjon og rapport om rammeverket (Art. 16(2))

8 kjernekrav i DORA-forordning

- Ha et **solid og dokumentert IKT-risikostyringsrammeverk**
- **Kontinuerlig overvåke** sikkerhet og funksjonalitet i alle IKT-systemer
- **Redusere IKT-risiko** gjennom robust, oppdatert og behovstilpasset teknologi og prosesser
- **Raskt oppdage og håndtere** kilder til IKT-risiko, avvik og sikkerhetsanomalier
- **Identifisere og følge opp** vesentlige avhengigheter til kritiske IKT-tredjepartsleverandører
- **Sikre kontinuitet** i kritiske og viktige funksjoner gjennom egnede business-continuity-tiltak (minst backup og gjenoppretting)
- **Regelmessig teste** planer og kontroller med hyppighet og omfang tilpasset risiko
- **Implementere læringspunkter** fra hendelser og tester, og opprettholde tilpasset IKT-sikkerhetsbevissthet og opplæring

DORA-RTS – NIVÅ 2

Ledelsesorganet / Management body

- Begrepet **management body** brukes flere steder i DORA-regelverket, og DORA legger et tydelig og omfattende ansvar på det som vi på norsk omtaler som **ledelsesorganet**.
- I lovproposisjonen til DORA-loven fastslås det at begrepet ledelsesorganet skal forstås som styret og daglig leder
  - **Daglig leder** - ansvar for den operative virksomheten
  - **Styret** - ansvar for forsvarlig organisering og tilsyn med virksomheten.

→ Dersom ansvarsfordelingen mellom styret og daglig leder ikke fremgår klart av norsk selskapsrett eller sektorregelverket, må styret sørge for en avklaring.

Artikkel 28 – Styring og organisering - Hovedpunkter

- Ledelsesorganet har det overordnede ansvaret for å etablere rammeverket for styring og kontroll
- Ledelsesorganet skal fastsette foretakets rapporteringsordninger om informasjonssikkerhet og digital operasjonell motstandsdyktighet
- I artikkel 28 framgår videre kravene om å fastsette klare roller, årlig beslutning om budsjett og de forhold som utdypes i artiklene 30 til 40
- Oppgavene knyttet til kontroll av etterlevelsen av kravene til IKT-risikostyring av IKT-tjenester kan utkontrakteres. NB! Det er likevel foretaket som er fullt ut ansvarlig for kravene til IKT-risikostyring overholdes.

Noen sentrale kontrollspørsmål

- Kan dere vise dokumentasjon på ledelsesorganets godkjenning av rammeverket siste 12, eller x måneder?
- Foretas det risikorapportering, og hvilken frekvens har rapporteringen
- Hva er budsjettet for å ivareta digital operasjonell motstandsdyktighet?
- Hvilken opplæring i IKT-sikkerhet/digital motstandsdyktighet er avholdt, og hva er planene videre?

Artikkel 28 – Styring og organisering - Kontroll og internrevisjon

- Foretaket skal sikre en hensiktsmessig atskillelse av og uavhengighet for kontrollfunksjoner og internrevisjonsfunksjoner
- Rammeverket skal revideres av internrevisjon i tråd med foretakets revisjonsplan
- Internrevisor skal
  - ha tilstrekkelige kunnskaper og ferdigheter og tilstrekkelig ekspertise med hensyn til IKT-risiko
  - være uavhengig
- Hyppigheten på revisjoner skal baseres på foretakets IKT-risiko

Artikkel 29 – Retningslinjer og tiltak for informasjonssikkerhet

- Foretaket skal etablere overordnede retningslinjer for informasjonssikkerhet (informasjonssikkerhetspolicy) som skal spesifisere de overordnede prinsippene og reglene for å beskytte fortrolighet, integritet, tilgjengelighet og autentisitet for data og IKT-tjenester
- På grunnlag av foretakets informasjonssikkerhetspolicy skal det fastsettes og implementeres IKT-sikkerhetstiltak for å redusere eksponering for IKT-risiko
- IKT-tiltakene omhandlet i artikkel 30–38 skal ivaretas

- **Noen sentrale kontrollspørsmål**
  - Er policyen oppdatert, godkjent og eksplisitt koblet til kravene i artikkel 30–38?
  - Hvordan viser dere sporbarhet fra policy til faktisk implementerte kontroller?
  - Er policyen kjent og etterlevd blant nøkkelpersonell?

Artikkel 30 – Klassifisering av informasjonsressurser og IKT-ressurser

- Alle kritiske og viktige funksjoner og tilhørende ressurser skal identifiseres, klassifiseres og dokumenteres
- Innbyrdes avhengigheter mellom ressursene skal kartlegges og oppdateres ved behov
- Tredjepartsstøttede kritiske funksjoner skal spesielt identifiseres og dokumenteres

- **Noen sentrale kontrollspørsmål**
  - Er alle kritiske funksjoner og tredjepartsavhengigheter identifisert og dokumentert?
  - Kan dere vise oversikt over tredjepartsavhengigheter?
  - Når ble klassifiseringen sist gjennomgått og oppdatert? Er klassifiseringen oppdatert etter siste store leverandørbytte?
  - Hvordan brukes klassifiseringer til å prioritere kontroller og tiltak?

Artikkel 31 – IKT-risikostyring

- **Foretaket skal**
  - fastsette risikotoleransenivåer for IKT-risiko i tråd med virksomhetens risikovillighet/risikoappetitt
  - kontinuerlig overvåke trusler og sårbarheter
  - identifisere og periodisk vurdere alle IKT-relaterte risikoer
  - med jevne mellomrom gjennomføre og dokumentere en IKT-risikovurdering som står i rimelig forhold til foretakets IKT-risikoprofil
  - fastsette risikoreduserende tiltak for IKT-risikoer utenfor risikotoleransen, og effektiviteten av disse tiltakene skal overvåkes og justeres ved behov

- **Noen sentrale kontrollspørsmål**
  - Er det prosess for kontinuerlig trussel- og sårbarhetsovervåking?
  - Er risikotoleransenivåene dokumentert og brukt i beslutninger? Hvem definerer konkrete risikotoleransenivåer for IKT-risiko?
  - Hvordan følges risikoer utenfor toleranse opp med tiltak? Kan dere vise et eksempel på tiltak som ble iverksatt etter risikovurdering?

Artikkel 32 – Fysisk sikkerhet og miljøsikkerhet

- Fysiske sikkerhetstiltak skal identifiseres og etableres basert på trusselbilde og klassifisering
- Lokaler og datasentre skal beskyttes mot uautorisert tilgang, angrep og miljøtrusler

- **Noen sentrale kontrollspørsmål**
  - Er fysiske tiltak risikobasert og dokumentert for relevante lokasjoner?
  - Hvordan er adgangskontroll og miljøbeskyttelse verifisert?
  - Er tredjepartsleverandørers fysiske sikkerhet vurdert?

Artikkel 33 – Tilgangskontroll

- Tilgangsrettigheter skal forvaltes etter "least privilege" og "need-to-know"-prinsippet

Prinsipp	Kort forklaring på norsk	Hovedpoeng	Typisk bruksområde
Least Privilege	Minste privilegium	En bruker/prosess får kun de rettigheter den absolutt trenger for å utføre sin jobb – ikke mer	Operativsystem, applikasjoner, sky-tjenester, admin-kontoer
Need-to-know	Behov for å vite	En person får kun tilgang til den informasjonen hun faktisk trenger for å gjøre jobben sin	Klassifisert informasjon, sensitive data, HR-saker, etterretning

- Autentiseringsmetoder skal være risikobaserte og sterke der det kreves
- Periodisk gjennomgang og håndtering av privilegerte tilganger skal gjennomføres

- **Noen sentrale kontrollspørsmål**
  - Brukes multifaktor-autentisering konsekvent på kritiske systemer?
  - Er periodisk tilgangsrevisjon gjennomført og dokumentert?
    Kan dere vise protokoll fra siste tilgangsrevisjon, og hvordan blir denne behandlet?
  - Hvordan håndteres og logges privilegerte/hastetilganger?

Artikkel 34 – Sikkerhet for IKT-virksomheten

- Livssyklusstyring av IKT-ressurser (anskaffelse, drift, vedlikehold, oppgraderinger og utfasing)
- Kapasitetsstyring og oppetid (tilgjengelighet)
- Automatisert sårbarhetsskanning, der utbedring gjennomføres risikobasert
- Sårbarhetsstyring og håndtering av utdatert teknologi

Noen sentrale kontrollspørsmål

- Har man en oversikt over IKT-eiendeler (utstyr, maskinvare, systemer og tjenester) i et eiendelsregister (Configuration Management Data Base (CMDB)).
- Har man oppmerksomhet og kontroll med utstyr, systemer, tjenester og maskinutstyr ikke automatisk lar seg integrere i CMDB automatisk.? Hva med utstyr hos tredjeparter?
- Har foretaket klassifisert IKT-eiendeler. Er man i stand til å identifisere de kritiske systemene (kfr. Art. 30)? Hvordan prioriteres og dokumenteres sårbarhetsutbedring? Kan dere vise siste sårbarhetsrapport og lukking av kritiske funn?
- Er logging implementert og foretas analyser på kritiske systemer?
- Hvordan håndteres risiko fra utdaterte komponenter?

Artikkel 35 – Data-, system- og nettsikkerhet

- Data skal beskyttes under lagring, under overføring og i bruk med hensiktsmessige tiltak
- Sikring av programvare, lagringsmedier og endepunkter
- Nettverk og tilkoblinger skal sikres mot uautorisert aktivitet
- Sikker sletting, avhending av utstyr og sikkerhetstiltak for fjernarbeid må implementeres

- **Noen sentrale kontrollspørsmål**
  - Hvilke krypteringsløsninger brukes på data i transitt og hvile? Kan dere vise hvilke systemer som har kryptering i hvile?
  - Hvordan er nettverkssikkerhet og segmentering dokumentert?
  - Er risiko ved fjernarbeid og private enheter kontrollert?

Artikkel 36 – IKT-sikkerhetstesting

- Har bestemmelser om å utarbeide og gjennomføre en strukturert risikobasert plan for IKT-sikkerhetstesting der foretakets identifiserte trusler og sårbarheter inkluderes
- Effektiviteten av sentrale sikkerhetstiltak skal valideres gjennom testing
- Testresultater skal føre til rask utbedring av kritiske funn

- **Noen sentrale kontrollspørsmål**
  - Finnes det en risikobasert testplan for kritiske systemer?
  - Er siste testresultater dokumentert og funn fulgt opp? Kan dere vise siste penetrasjonstest og tiltaksplan?
  - Hvordan prioriteres og lukkes kritiske testfunn?

Artikkel 37 – Anskaffelse, utvikling og vedlikehold av IKT-systemer

- Foretaket skal, når det er hensiktsmessig, utarbeide og implementere en risikobasert prosedyre for anskaffelse, utvikling og vedlikehold av IKT-systemer.
- Prosedyren skal sørge for at alle krav dokumenteres og godkjennes, inkludert sikkerhetskrav
- Prosedyren må sikre at alle IKT-systemer testes før de tas i bruk for første gang, og at testing også foregår når det utføres endringer som kan påvirke produksjonsmiljøet
- Prosedyren skal sikre at nødvendige sikkerhetstiltak identifiseres og implementeres for å beskytte systemene under utvikling og implementering

- **Noen sentrale kontrollspørsmål**
  - Er sikkerhetskrav integrert i anskaffelsesprosessen? Hvordan ble disse besluttet?
  - Kan dere vise kravspesifikasjon og testprotokoll fra siste store innkjøp?
  - Hvordan gjennomføres testing før produksjonssetting?
  - Er tiltak mot utilsiktet endring dokumentert?

Artikkel 38 – Styring av IKT-prosjekter og håndtering av IKT-endringer

- Prosedyre for styring av IKT-prosjekter
- Prosedyre for håndtering av IKT-endringer

- **Noen sentrale kontrollspørsmål**
  - Er det en dokumentert prosess for endringshåndtering med testing? Kan dere vise endringslogg og testdokumentasjon fra siste store endring?
  - Hvordan sikres testing og rollback på kritiske endringer?
  - Er større prosjekter styrt med definerte roller og faser?
  - Har dere dokumentasjon på at endringer faktisk testes og godkjennes (spesielt ved kritiske systemer)

Artikkel 39 – Komponenter i planen for IKT-kontinuitet i virksomheten

- Planen skal (her er noen eksempler, de detaljerte kravene fremgår i artikkelen)
  - være godkjent av ledelsesorganet (management body).
  - være dokumentert og lett tilgjengelig i nød- og krisesituasjoner.
  - tildele tilstrekkelige ressurser (kompetanse, tid, verktøy og budsjett)
  - fastsette planlagte gjenopprettingskrav og tidsrammer
  - identifisere "utløsere" for når IKT-kontinuitetsplanen skal aktiveres
  - …
  - vurdere alternativer der gjenoppretting ikke er mulig på kort sikt
  - ….
  - oppdateres i tråd med erfaringer fra hendelser og tester, nye risikoer og trusler m.fl (Kontinuerlig forbedring og endringsstyring).

- **Noen sentrale kontrollspørsmål**
  - Er RTO og RPO definert for kritiske funksjoner? Hva er RTO og RPO for deres kjernebank- eller kundesystem?
  - Hvordan er kritiske tredjepartsavhengigheter håndtert?
  - Er sikkerhetskopiering tilpasset kritikalitet?
  - Hvem informerer man ved ulike typer kriser – internt og eksternt, og hvordan informeres kundene?

Artikkel 40 – Testing av planene for kontinuitet i virksomheten

- **Årlig** og hendelsesbasert testing av kontinuitetsplanene
- Formålet med testene – validering av gjennomførbarhet og identifisering av mangler
- Dokumentasjon, håndtering og rapportering av funn

- **Noen sentrale kontrollspørsmål**
  - Er backup- og gjenopprettingstest gjennomført årlig?
  - Hvordan følges de identifisert manglene fra testing opp frem til at de lukkes?
  - Er gjenoppretting testet innen definerte RTO/RPO? Kan dere vise protokoll fra siste gjenopprettingstest?

Artikkel 41 – Format på og innhold i rapporten om gjennomgåelsen av det forenklede rammeverket for IKT-risikostyring

- Artikkel 41 etablerer et omfattende og strukturert kravsett til rapportering.
- Rapporten som utarbeides skal:
  - være søkbar
  - gi en helhetlig situasjonsbeskrivelse av IKT-risiko
  - dokumentere årsaker, funn og analyse
  - vise modenhet, kontroll og forbedringstiltak
  - være ledelsesforankret
  - sikre sporbarhet mot tidligere rapporter og historikk

- **Noen sentrale kontrollspørsmål**
  - Er det utarbeidet en gjennomgangsrapport som dekker alle elementer? Kan dere sende siste rapport om gjennomgang av rammeverket?
  - Hvordan følges tiltak og tidligere svakheter opp?
  - Er rapporten brukt i dialog med ledelse og tilsyn?

FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Kunne du tenke deg å jobbe i Finanstilsynet?

finanstilsynet.no/jobb-hos-oss