FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DORA

6. november

❑ Regelverket – innledning	Olav og Ida
❑ Styring av IKT-risiko	Jarleif
❑ Håndtering av hendelser	Olav
❑ Testing av digital motstandsdyktighet	Arild
❑ Benstrekk (ca. 10 min)	
❑ Styring av tredjepartsrisiko	Stig og Olav
❑ Deling av informasjon inkl. evt. NFCERT	Ida og Morten
❑ Hva bør foretakene forberede seg på	Olav
❑ Kommende DORA-webinarer	Olav
❑ Spørsmål	Olav og Ida

Foredragsholderne


Ida Kvernebo Mackenzie


Jarleif Lødøen


Stig Ulstein


Arild Tømmerås


Olav Johannessen


Morten Tandle NFCERT

Regelverket - innledning

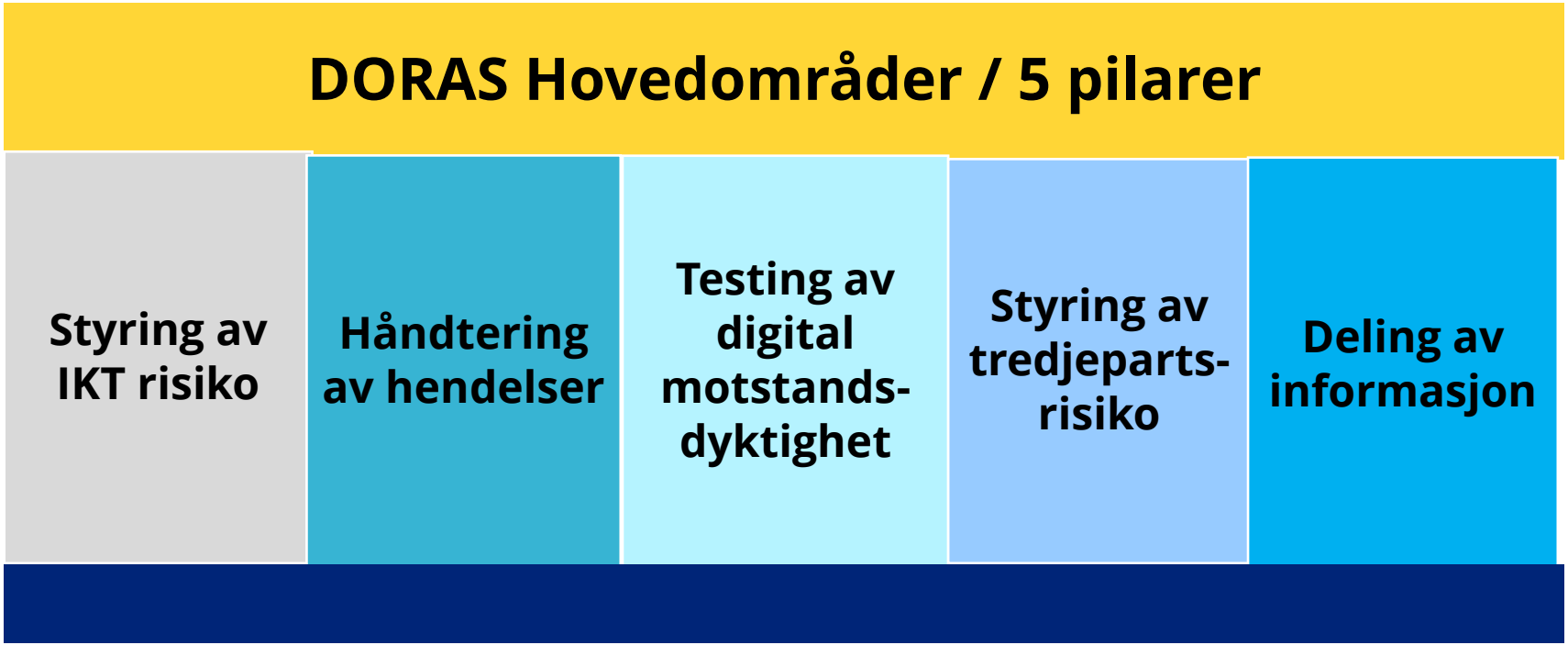
Fra forskrift om forretnings- og sparebankers bruk av datamaskiner og terminaler til DORA

- *Forskrift om forretnings- og sparebankers bruk av datamaskiner og terminaler 1983*
- *Forskrift om bruk av informasjonsteknologi (IT) 1993*
- *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) 2003*
- *Lov om tilsynet med finansforetak mv – meldeplikt utkontraktering 2014*
- *Forskrift om meldeplikt ved utkontraktering av virksomhet mv 2020*

- *CEBS Guidelines on Outsourcing 2006*
- *Forarbeider om utarbeidelse av felles retningslinjer for IKT-sikkerhet for banker (EBA) 2014-2017*
- *Guidelines on security measures for operational and security risks (PSD2) 2017*
- *Recommandation outsourcing to cloud service providers EBA 2017*
- *Guidelines on ICT and security risk management EBA 2019*
- *Guidelines on outsourcing arrangements EBA 2019*
- *Guidelines on outsourcing to cloud service providers EIOPA 2020*
- *Guidelines on information and communication technology security and governance EIOPA 2020*
- *Guidelines on outsourcing to cloud service providers ESMA 2020*

+++ *flere EU-sektorregelverk med IKT-bestemmelser*

DORA HOVEDOMRÅDER



Endringsbestemmelser - Direktiv + DORA

Forordningen skal «monteres» inn i en rekke eksisterende direktiver og forordninger

- **Endring i** operasjonelle risiko- eller risikostyringskrav i **direktiver**

  Krysshenvisninger

2009/65/EC	UCITS, kollektiv investering i omsettelige verdipapirer
2009/138/EU	SOLVENS II, forsikring og reassuranse
2011/61/EU	AIFMD, alternative investeringsfondforvaltere
EU/2016/2341	IORP - tjenestepensjon

  IKT-relaterte bestemmelser

EU/2013/36	CRD, Kapitaldekning - banker mm -
2014/65/EU	MIFID2 - finansielle instrumenter
(EU) 2015/2366	PSD2 – betalingstjenester og -foretak

- **Endringer i forordninger (**«Amendments» i DORA-forordningen)

(EC) No 1060/2009	Kredittvurderingsbyråforordningen, CRA
(EU) No 648/2012	Forordn. OTC-derivater, sentrale motparter og trans.registre, EMIR
(EU) No 909/2014	Verdipapirsentralforordningen, CSDR
(EU) 2016/1011	Referanseverdiforordningen, BMR
Amd. Reg. (EU) No 600/2014	Verdipapirmarkedsforordningen, MiFIR

- Samtidig implementering

Fra IKT-forskriften til DORA

DORA	IKT-forskriften *(+ VP-register-loven)*
Governance	§ 2 Organisering + (Foretaksregelverk)
Styring av IKT-risiko	§ 3 Risikoanalyse, § 4 Kvalitet, § 5 Sikkerhet, § 8 Drift, § 9 mhp Endringshåndtering, § 11 Driftsavbrudd og kriseberedskap, § 12 Utkontraktering, § 13 Dokumentasjon
Håndtering av hendelser	§ 9 Avviks- og endringshåndtering
Testing av digital motstands-dyktighet	§ 11 Driftsavbrudd og kriseberedskap
Styring av tredjeparts- risiko	§ 12 Utkontraktering, § 2 Organisering
Deling av informasjon og etterretning ift. cybertrusler og sårbarheter	Samhandling med/gjennom NFCERT
Bestemmelser for myndighetene, bl.a. om samarbeid, sektorovergripende beredskapstesting og sanksjoner	

Proporsjonalitet

Momenter:

- ❑ Størrelse
- ❑ Risikoprofil
- ❑ Art, omfanget av og kompleksiteten i foretakets
  - Tjenester
  - Aktiviteter
  - Drift

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))

Implementering i Norge

- Lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven):
  - Parallelt løp med EØS-avtalen
  - Proposisjon under arbeid
  - Stortingsvedtak
  - Når trer loven i kraft?

- Hva med nivå2-regelverket?
  - Hjemmel for fastsettelse i forskrift
  - Førtidige implementeringer?
  - Høringer?

Styring av IKT-risiko

Rammeverk for risikostyring

- Avsnitt I dekker styring og kontroll og organisering: (Artikkel 5 - Governance and Organisation)
- Avsnitt II omfatter
  - Artikkel 6 – 14 – Detaljtemaer
    - Artikkel 6: IKT-risikostyringsrammeverk (ICT Risk Management Framework)
    - Artikkel 7: IKT-systemer, protokoller og verktøy (ICT Systems, Protocols and Tools)
    - Artikkel 8: Identifikasjon (Identification)
    - Artikkel 9: Beskyttelse og forebygging (Protection and Prevention)
    - Artikkel 10: Deteksjon (Detection)
    - Artikkel 11: Respons og gjenoppretting (Response and Recovery)
    - Artikkel 12: Backup-policyer og prosedyrer, gjenopprettingsprosedyrer og metoder
    - Artikkel 13: Læring og utvikling (Learning and Evolving)
    - Artikkel 14: Kommunikasjon (Communication)
  - Artikkel 15 og 16 – Temaer som ikke gås gjennom i detalj
    - Artikkel 15: Videre harmonisering av IKT-risikostyringsverktøy, metoder, prosesser og policyer
    - Artikkel 16: Forenklet IKT-risikostyringsrammeverk for noen grupper av foretak

→ *RTS: "Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework"*

Artikkel 5 - Governance and organisation

- Tema: Styre og kontrollere IKT-risiko der ledelsen/styret har det overordnede ansvaret
- Oppsummert:
  - Krav om å etablere et internt styrings- og kontrollrammeverk for effektiv og forsvarlig håndtering av IKT-risiko (for å oppnå høy digital operasjonell motstandsdyktighet).
  - Ledelsen/styret har ansvaret for implementering av IKT-risikostyringsrammeverket
  - Ledelsen/styret skal fastsette og godkjenne strategier for digital operasjonell motstandsdyktighet, gå gjennom og vurdere IKT-forretningskontinuitet, fastsette internrevisjons-aktiviteter, fastsette opplæringsprogrammer, og sikre tilstrekkelig finansielle- og personellmessige ressurser for å innfri kravene til digital operasjonell motstandsevne (DOR).
  - Tilleggskrav som er verdt å merke seg
    - Etablere en rolle for å overvåke risiko knyttet IKT-tredjeparts tjenesteleveranser.
    - Sikre at medlemmer av ledelsen/styret til enhver tid har tilstrekkelig kunnskap og ferdigheter for å kunne forstå og vurdere IKT-risiko ift. forretningsrisiko.

Artikkel 6 - ICT Risk Management Framework (1)

- Tema: Utarbeide et helhetlig og godt dokumentert IKT-risikostyringsrammeverk som inngår i foretakets overordnede risikostyringssystem.
- Oppsummert:
  - Strategier, policyer, prosedyrer, IKT-protokoller og verktøy for å beskytte alle informasjons- og IKT-ressurser.
  - Rammeverket skal være dokumentert og skal revideres periodisk
  - Med utgangspunkt i IKT-risikostyringsrammeverk er målet å minimere konsekvensen av IKT-risiko
  - Håndtering og overvåkning av IKT-risiko skal tildeles en «independent» kontrollfunksjon
  - Foretaket skal fastsette akseptabel IKT-risiko, inkludert analyser av hvilke IKT-avvik man kan tolerere
  - Verifikasjon av etterlevelsen av IKT-risikostyringen kan utkontrakteres til enheter i eget foretak (intragroup), eller til eksterne
  - DOR-strategi for hvordan IKT-risikostyringsrammeverket skal implementeres (Se neste side)

Artikkel 6 - ICT Risk Management Framework (2)

- Oppsummering forts… Strategi for hvordan IKT-risikostyringsrammeverket skal implementeres
  - Strategien skal inkludere metoder for å håndtere IKT-risiko og nå spesifikke IKT-mål ved å:
    - forklare hvordan rammeverket støtter foretakets forretningsstrategi og mål
    - etablere risikotoleransenivået for IKT-risiko i samsvar med foretakets risiko-apetitt, inkludert toleransenivået for IKT-avbrudd
    - sette klare mål for informasjonssikkerhet
    - beskrive IKT-arkitekturen og evt. hvilke endringer som må til for å nå spesifikke forretningsmål
    - beskrive mekanismene for å oppdage IKT-relaterte hendelser, forhindre konsekvenser og gi beskyttelse mot dem
    - dokumentere den nåværende situasjonen for digital operasjonell motstandsdyktighet med utgangspunkt i antall rapporterte større IKT-relaterte hendelser og effektiviteten til forebyggende tiltak
    - implementere test av digital operasjonell motstandsdyktighet i samsvar med kapittel IV i denne forordningen;
    - beskrive en kommunikasjonsstrategi i tilfelle IKT-relaterte hendelser som krever offentliggjøring i henhold til artikkel 14.

Artikkel 7: ICT Systems, Protocols and Tools

- Tema: Bruk og vedlikehold av oppdaterte IKT-systemer, protokoller og verktøy.

- Oppsummert:
  - For å adressere og håndtere IKT-risiko må foretaket sikre at de har oppdaterte IKT-systemer, protokoller og verktøy.
  - Systemene forutsettes å være tilpasset virksomheten omfang, at de er teknologisk motstandsdyktige og at de har kapasitet til å håndtere situasjoner med behov for ekstra behandlingskapasitet

Artikkel 8: Identification

- Tema: Identifikasjon og dokumentasjon av alle IKT-støttede forretningsfunksjoner.
- Oppsummert:
  - Identifisere, klassifisere og dokumentere alle IKT-støttede forretningsfunksjoner, roller og ansvar (minimum årlig, eller ved behov)
  - Identifisere, klassifisere og dokumentere de informasjons- og IKT-ressurser som støtter disse funksjonene, også på også på eksterne lokasjoner (minimum årlig, eller ved behov).
  - Kartlegg konfigurasjon og koblingene og avhengighetene for de de informasjons- og IKT-ressurser som anses som kritiske.
  - Identifiser og dokumenter alle prosesser som er avhengige av IKT-tjenesteleverandører, og identifiser de som støtter kritiske eller viktige funksjoner
  - Løpende identifisering av alle kilder til IKT-risiko, og periodisk vurdering relevante scenarioer for cybertrusler og IKT-sårbarheter (minimum årlig, eller ved behov)
  - Gjennomføre risikovurdering ved hver større IKT-endring
  - Vedlikeholde ovennevnte oversikter og oppdater disse periodisk, og ved større endringer
  - Periodisk risikovurdering av fagsystemene (minst årlig) og før/etter man kobler til ny teknologi, applikasjon eller system

Artikkel 9: Protection and Prevention (1)

- Tema: Kontinuerlig overvåking og kontroll av sikkerheten og funksjonaliteten til IKT-systemer.
- Oppsummering:
  - Kontinuerlig overvåke og kontrollere sikkerheten og funksjonaliteten til IKT-systemer for å minimere konsekvensen av IKT-risiko.
  - Utvikle, anskaffe og implementere IKT-sikkerhetspolicyer, prosedyrer, protokoller og verktøy for motstandsdyktighet, kontinuitet og tilgjengelighet for IKT-systemene
  - Foretaket må sikre at IT-løsningene og prosessene ivaretar sikkerheten proporsjonalt ift. risiko (risikobasert);

Artikkel 9: Protection and Prevention (2)

- Oppsummering forts…
  - Som del av IKT-risikorammeverket skal det utvikles
    - Informasjonssikkerhetspolicy
    - Robust forvaltningsstruktur for nettverk- og infrastruktur for øvrig
    - Policyer som begrenser fysisk eller logisk tilgang til informasjons og IKT-ressurser
    - Policyer, prosedyrer og kontroller for tilgangsstyring og forsvarlig administrasjon av disse
    - Policyer og protokoller for sterke autentiseringsmekanismer
    - Policyer og protokoller for beskyttelsestiltak ved anvendelse av kryptografiske nøkler
    - Dokumenterte policyer, prosedyrer og kontroller for IKT-endringsstyring
    - Hensiktsmessige og dokumenterte policyer for oppdatering og patching

Artikkel 10: Detection

- Tema: Mekanismer for å oppdage unormale aktiviteter og IKT-relaterte hendelser.

- Oppsummering:
  - Etablere mekanismer for å raskt oppdage unormale aktiviteter
  - Mekanismene må testes regelmessig
  - Foretaket nå sørge for å avsette tilstrekkelige ressurser og kapabiliteter for å overvåke brukeraktivitet, forekomsten av IKT-anomalier og IKT-relaterte hendelser (spesielt cyberhendelser)
  - Datainnsamlingstjenesteleverandører er behandlet særskilt

Artikkel 11: Response and Recovery (1)

- Tema: IKT-forretningskontinuitetspolicy og respons- og gjenopprettingsplaner.
- Oppsummering:
  - Som del av IKT-risikostyringsrammeverket skal foretaket etablere en IKT-forretningskontinuitetspolicy
  - Som del av IKT-risikostyringsrammeverket, skal finansielle enheter implementere IKT-respons- og gjenopprettingsplaner (disse er gjenstand for uavhengige intern revisjon)
  - Foretak skal etablere, vedlikeholde og periodisk teste IKT-forretningskontinuitetsplaner for kritiske og viktige funksjoner som er utkontraktert
  - Det skal gjennomføres en analyse av konsekvenser ved avbrudd i foretakets tjenesteleveranser (BIA)
  - Foretaket skal teste IKT-forretningskontinuitetsplaner og IKT-respons- og gjenopprettingsplanene årlig, samt ved større endringer i IKT-systemer og funksjoner som støtter kritiske eller viktige funksjoner;

Artikkel 11: Response and Recovery (2)

- Oppsummering forts…
  - Foretaket skal ha en krisehåndteringsfunksjon
  - Ved avvikshendelser bør foretaket dokumentere om hva som skjer før og når en hendelse pågår, slik at det finnes grunnlag for å analysere og forbedre planer og prosedyrer ved lignende fremtidige hendelser
  - Særskilt krav: verdipapirregistre skal gi kompetente myndigheter kopi av resultatene av IKT-forretningskontinuitetstestene, eller lignende øvelser
  - Foretak skal på forespørsel kunne rapportere et estimat på samlede årlige kostnader og tap forårsaket av store IKT-relaterte hendelser

Artikkel 12: Backup policies and procedures, restoration and recovery procedures and methods

- Hovedtema: Utvikling og dokumentasjon av backup-policyer og gjenopprettingsprosedyrer.

- Oppsummering:
  - For å sikre gjenoppretting av IKT-systemer og data med minimal nedetid, begrenset forstyrrelse og tap, skal IKT-risikostyringsrammeverket omfatte backup-policyer og prosedyrer, samt restore- og gjenopprettings prosedyrer og metoder
  - Foretaket må kunne opprettholde redundant IKT-kapasiteter for å sikre tjenesteleveransene ift. forretningsbehov
  - Beskytte av backup-/restore-fasiliteter for å unngå uautorisert aksess eller ødeleggelse

  - Spesielle krav for sentrale motparter, datainnsamlingsleverandører, og verdipapirregistre
  - Sikre at avtalte tjenestenivåer for kritiske eller viktige funksjoner utfra den potensielle innvirkningen på markeds effektivitet ivaretas ved fastsettelse av RTO/RPO
  - Ved gjenoppretting skal foretaket utføre nødvendige kontroller for å sikre dataintegritet

Artikkel 13: Learning and evolving

- Hovedtema: Læring og utvikling
- Oppsummering:
  - Foretaket skal ha kapasitet og personell for å innhente informasjon om sårbarheter, cybertrusler og IKT-relaterte hendelser (spesielt cyber-angrep), samt å analysere hvordan dette kan påvirke foretakets digitale operasjonell motstandsdyktighet.
  - Større IKT-relaterte hendelser skal vurderes/gjennomgås med tanke på å identifisere årsak, og mulige forbedringer, og på forespørsel kunne rapportere hvilke endringer som ble gjort etter at hendelsen inntraff.
  - Følge opp/ha kontroll med effektiviteten av strategien for digital operasjonell motstandsevne
  - Utvikle IKT-sikkerhetsbevissthetsprogrammer og opplæring i digital operasjonell motstandskraft som obligatoriske moduler i opplæringsprogrammer for ansatte
  - Kontinuerlig overvåke relevant teknologiske utvikling

Artikkel 14: Communication

- Tema: Kommunikasjonsplaner for offentliggjøring av informasjon for IKT-relaterte hendelser.
- Oppsummering:
  - Etablere krisekommunikasjonsplaner som sikrer en ansvarlig offentliggjøring av forhold forbundet med IKT-relaterte hendelser eller sårbarheter til kunder og motparter, samt til offentligheten, der det er hensiktsmessig
  - Kommunikasjonsretningslinjer for internt ansatte og for eksterne interessenter.
  - Én person i foretaket skal være ansvarlig for å implementere kommunikasjonsstrategien for IKT-relaterte hendelser og ivareta funksjonen for informasjon til offentlighet og media for dette formålet.

Artikkel 15: Further harmonisation of ICT risk management tools, methods, processes and policies

- Tema: Inneholder detaljer om hvilket andre nivå regelverk som skal utarbeides (RTS)

ANNEX: STATUS OF THE POLICY MANDATES

WG	Art	DORA policy work	ESA Lead	Scoping notes	ECB/ENISA involvement (1)	DL	Month
1	15	RTS on ICT risk management framework	ESMA	Agreed	ENISA (consulted)	Jan-24	12
1	16	RTS on simplified ICT risk management framework	ESMA	Agreed	ENISA (consulted)	Jan-24	12
1	28.1	RTS to specify the policy on ICT services performed by 3rd party	EBA	Agreed	na	Jan-24	12
1	30.5	RTS to specify elements when sub-contracting critical or important functions	EBA	Agreed	na	Jul-24	18
1	26.11	RTS to specify threat led penetration testing aspects	CA led	On-going	ECB (in agreement)	Jul-24	18
2	18.3	RTS on criteria for the classification of ICT-related incidents	EBA	Agreed	ENISA and ECB (consulted)	Jan-24	12
2	20.a	RTS on specifying the reporting of major ICT-related incidents	EBA	Agreed	ENISA and ECB (consulted)	Jul-24	18
2	20.b	ITS to establish the reporting details for major ICT-related incidents	EBA	Agreed	ENISA and ECB (consulted)	Jul-24	18
2	11.11	Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents	EBA	Agreed	na	Jul-24	18
2	21	Feasibility report on single EU Hub for major ICT-related events	ESMA	On-going	ENISA and ECB (consulted)	Jan-25	18 (3)
2	Na	ESRB recommendation - interim A(1) and B	EIOPA	Agreed	ECB and ESRB (together)	Jul-23	6
3	28.9	ITS to establish the templates for the Register of information	EIOPA	Agreed	na	Jan-24	12
3	31.8	Call for advice on criticality criteria	EIOPA	N/A	na	Sep-23	9
3	43.2	Call for advice on oversight fees	ESMA	N/A	na	Sep-23	9
3	32.7	GL on cooperation between ESAs and CAs regarding the structure of the oversight	EIOPA	On-going	na	Jul-24	18

Artikkel 16: Simplified ICT risk management framework

- Tema: Forenklet rammeverk for IKT-risikostyring i noen grupper av foretak

- Oppsummering:
  - Artiklene 5 til 15 gjelder ikke for enkelte typer små foretak som angitt i artikkel 16.
  - Temaer knyttet risikostyringen i disse små foretakene vil vi komme tilbake til på et senere seminar når nivå 2- regelverket (RTS) blir presentert
  - Dersom det er spesifikke spørsmål som ønskes belyst på senere seminar så kan dette deles i chat eller som oppgitt i innkallingen til dette seminaret

Håndtering av hendelser

Håndtering av hendelser

- Prosess for å håndtere hendelser
- Oversikt over alle hendelser
- Rapportering av hendelser
- Kostnadsvurderinger
- Cyber trusler
- Betalingsrelaterte hendelser
- Rapporteringsmaler
- EU-SCICF

Testing av digital motstands-dyktighet

Generell sikkerhetstesting

- **Formål**: Styrke digital forsvarsevne i finanssektoren ved å avdekke svakheter eller mangler i foretakenes digitale motstandsdyktighet
- **Krav**: Foretakene skal ha et program for risikobaserte tester som en del av rammeverket for IKT-risikostyring
- **Proporsjonalitet**: Krav til testing bygger på et proporsjonalitetsprinsipp, som tar hensyn til forskjeller mellom foretak når det gjelder risikoprofil, størrelse og kompleksitet
- **Hyppighet**: Generelle sikkerhetstester skal gjennomføres regelmessig (årlig) og resultatene skal følges opp

Generell sikkerhetstesting- innhold

- Foretak skal med utgangspunkt i egen risikoprofil vurdere hvilke testmetoder som vil dekke eget behov for generell sikkerhetstesting

- Eksempler på metoder som det forventes at foretak vurderer/benytter:
  - sårbarhetsvurderinger, nettverkssikkerhetsvurderinger, gap-analyser, fysiske sikkerhetsgjennomganger, spørreskjemaer og skanningsløsninger, kildekodegjennomganger
  - scenariobaserte tester, ytelsestesting, ende-til-ende-testing, penetrasjonstesting

- Generell sikkerhetstesting i DORA er i stor grad dekket av dagens IKT-forskrift, men vil beskrive kravene mer i detalj

Avansert testing- TLPT

- **Kapittel 26** i EUs DORA-regulering omhandler avansert testing av IKT-verktøy, systemer og prosesser. Det kreves i utgangspunktet at finansforetak, med noen unntak, gjennomfører avansert testing via trusselbasert penetrasjonstesting (TLPT) minst hvert tredje år
- Basert på risikoprofilen til den finansielle enheten, kan kompetent myndighet be en finansiell enhet om å redusere eller øke frekvensen for testing
- Trusselbasert penetrasjonstesting er designet for å evaluere styrken på beskyttelsene og identifisere mulige sårbarheter i IKT-systemene, samt at testgjennomføringen skal valideres av relevante myndigheter

Styring av tredjepartsrisiko

Styring av tredjepartsrisiko

- Foretakene må inkludere risiko fra tredjeparts IKT-tjenester i sin overordnede IKT-risikostyring
- Foretakene må regelmessig gjennomgå og oppdatere strategier for å håndtere IKT-risiko
- Avtaler med tredjeparts IKT-leverandører må oppfylle foretakenes krav til sikkerhet samt beredskapsplaner.

Styring av tredjepartsrisiko - viktige forhold

- Regelmessig gjennomgå risiko identifisert i bruk av IKT-tjenester
- Sørge for at avtaler med IKT-tjenesteleverandører oppfyller sikkerhetsstandarder
- Implementere exit-strategier og beredskapstiltak for kritiske IKT-tjenester
- Vurdere risiko knyttet til konsentrasjon av IKT-tjenester

IKT-tjenesteavtaler - register

- Finansielle enheter må vedlikeholde og oppdatere en register over alle kontraktsmessige avtaler med IKT-tredjepartsleverandører på enhets-, subkonsolidert og konsolidert nivå
- Registeret skal skille mellom avtaler som dekker kritiske eller viktige funksjoner og de som ikke gjør det
- Finansielle enheter skal rapportere årlig til tilsynsmyndighetene om nye avtaler, kategorier av leverandører, og typer av IKT-tjenester som leveres

IKT-tjenesteavtaler – i tråd med regelverket

- Foretak og IKT-tjenesteleverandører må tydelig definere sine rettigheter og forpliktelser skriftlig
- Avtalene må inkludere detaljer om tjenestenivåer, sikkerhetstiltak, og beredskapsplaner
- Det er også krav om at leverandørene skal samarbeide med myndigheter og bistå ved IKT-hendelser uten ekstra kostnad

Oversight

- De europeiske tilsynsmyndighetene (ESAs) skal vurdere og utpeke IKT-tredjepartsleverandører som kritiske basert på kriterier som systemisk påvirkning og avhengighet.
- Utpekte leverandører må oppfylle spesifikke krav og samarbeide med tilsynsmyndighetene.
- Finansielle enheter må sikre at de kun bruker tjenester fra kritiske leverandører som har etablert en filial i EU senest 12 måneder etter utpekingen.

IKT-tjenesteavtaler – Etterlevelse

Når må IKT-tjenesteavtalene være i samsvar med regelverket

- ❑ DORA's krav er kjent
- ❑ Oversikt over alle avtaler
- ❑ Plan for fornyelse
- ❑ Vurdere avtalens kritikalitet og varighet/løpetid
- ❑ Så raskt som mulig

Deling av informasjon

Deling med myndigheter under NIS2 (DORA art. 47)

NIS2-direktivet ((EU)2022/2555)

- ❑ Et generelt digitalsikkerhetsdirektiv NIS2-dirketivet
- ❑ Gjelder for tilbydere av samfunnsviktige tjenester
- ❑ Gjelder flere sektorer i tillegg til deler av finanssektoren (eks. energi og transport)

Myndigheter under NIS2

- ❑ Cooperation Group = En overnasjonal gruppe
- ❑ CSIRT (Computer Security Incident Response Team) = NSM/NCSC

Deling med andre tilsynsmyndigheter og ECB

Mellom tilsynsmyndigheter (art. 48)

- Tilsynsmyndighetene skal samarbeide seg i mellom
- Tilsynsmyndighetene skal samarbeide med Lead Overseer
  - Herunder dele informasjon om kritiske IKT-tjenesteleverandører til Lead Overseer

Mellom tilsynsmyndigheter, ESA'ene og ECB (art. 49 nr.2)

- Formål: Bidra til lik praksis – reglene for kommunikasjon og sanksjoner (art. 47-54)

Deling mellom foretak (art. 45)

- Deling av informasjon er tillatt på nærmere vilkår
- Foretak som deltar i fora for informasjonsdeling må melde det til Finanstilsynet.

Kort intro - Nordic Financial CERT

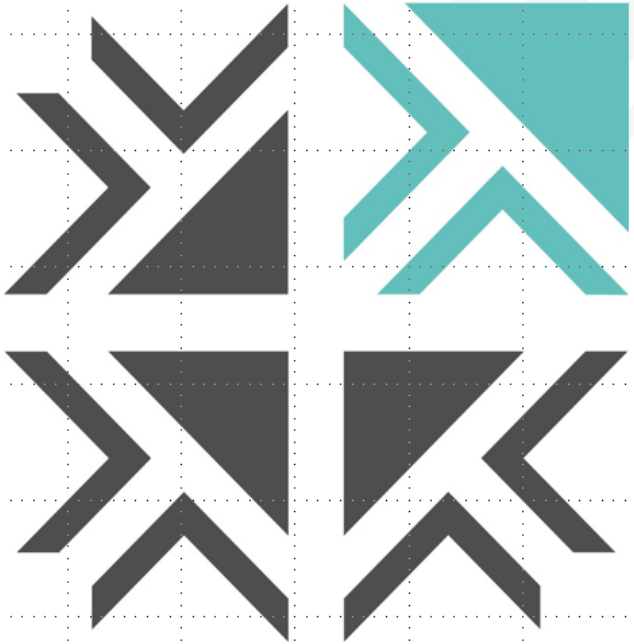
- Non-profit forening, med 240+ medlemmer i de 5 nordiske landene
  - Banker, forsikring, pensjon m.fl

- Hub for deling og samarbeid
  - Mellom medlemmer
  - Privat/offentlig (Politi, tilsyn o.a.)
- Fyller "operativ deling og situasjonsbilde" biten av SRM-rollen etter avtale med Finanstilsynet

Picture credit: Wikipedia

Hub for deling av data/informasjon og kunnskap

- Avtaleregulert
- Lukket/sikret
- Automatiserbart (APIer)
  - Digital delingsplattform
- Med community –
  dvs delegrupper av fagfolk



Dora artikkel 45

- NFCERT driver et delingscommunity som passer som hånd-i-hanske med informasjonsdeling slik det er beskrevet i Dora artikkel 45

- Hovedpoenget:
  - Angriperne deler og samarbeider
  - Vi som forsvarer trenger også å dele og samarbeide for å unngå at vi blir tatt «en og en»

Hovedelementene:

- Raise awareness in relation to cyber threats
- Share cyber threat information- and intelligence limiting or impeding the cyber threats' ability to spread
- Share cyber threat information- and intelligence supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages
- Share cyber threat information- and intelligence within trusted communities

Hva bør foretakene forberede seg på

Forberede

- IKT-forskrift og retningslinjer → Detaljert og omfattende regelverk
- DORAs krav
- Oppdatering av rammeverk, prosesser, policyer, rutiner, registerføring, etc
- Rammeverket for risikostyring
- Innvolvere og Ansvarliggjøre Styret og ledelsen
- Styre- og Ledelsesrapportering
- Leverandøroppfølging
- Resilience (motstandsdyktighet)
- Justeringer i organisasjonen

Forberede (forts.)

- Avtaler
- Verktøystøtte og IT-utvikling
- Kompetansetiltak
- Virksomhetsanalyser (Business Impact Analyses – BIA)
- Risikoappetitt
- Tre forsvarslinjer el. tilsvarende
- Samhandling styrke den digitale motstandsdyktigheten
- Nivå-2 regelverket

Kommende webinarer

Kommende webinarer

- Rapportering av hendelser
- Registerføring og rapportering av IKT-tjenesteavtaler
- Melding om nye IKT-tjenesteavtaler
- IKT-risiko
- Testing av digital motstandsdyktighet
- Konsern-tematikk

Spørsmål?

Mottatte spørsmål

1. Hva er forholdet mellom IKT-forskriften, EBA-retningslinjer og DORA?
2. Hva vil implementeringstidspunkt i Norge?
3. Hvordan vil implementeringstidspunkt påvirke foretak som har hovedkontor i Norge og filialer i EU?
4. Hva er deres tanker om overlapp med andre reguleringer og hva som vil få fortrinn ved konflikter mellom lovverk? (f.eks. GDPR og DORA)
5. Er det spesielle ting vi som et land utenfor EU bør forberede oss på?
6. Hvordan vil samarbeidet mellom myndigheter i Norge og andre EU-land være med tanke på grensekryssende arbeid? Vil det komme noen veiledning for eventuell jurisdiksjonell overlapp?
7. For EU var kravet om innsendelse av ROI satt til 17.jan (ikrafttredelses datoen), når vil ROI måtte sendes inn for norske selskaper, og skal dette gå via Finanstilsynet i Norge?
8. Hva er utgangspunktet for beregningen for aksessoriske agenter og forholdet til terskelverdiene for små og mellomstore entities? Den aksessoriske agentens hovedvirke eller virksomheten som aksessorisk agent? Det er store foretak (f eks bilforhandlere) som klart overstiger terskelverdiene om vi ser på hele virksomheten, men hvor forsikringsformidlingsvirksomheten faller under terskelverdiene. Omfattes slike foretak av DORA?

Mottatte spørsmål

9. Avklaring på hvilke IKT-tjenester som faller inn under DORAs definisjon (tjeneste som støtter eller muliggjør levering av finansielle tjenester via IKT-system), herunder videresalg av standardprodukter
10. Vil det lages en felles mal som foretakene kan bruke for innhenting av informasjon fra sine leverandører for utfylling av sitt Register of Information (RoI)?
11. Avklaring om hvem som vurderer hvilke underleverandører som effektivt understøtter IKT-tjenester som støtter kritiske eller viktige funksjoner eller vesentlig del av disse og som skal føres i RoI?
    - Er det foretaket som skal gjøre denne vurderingen for alle ledd i leverandørkjeden, eller «kaskaderes» dette ansvaret nedover i leverandørkjeden til den enkelte leverandør som foretar en eller flere utkontrakteringer?
    - Er det mer konkrete kriterier som kan/bør brukes for å identifisere leverandører som skal dokumenters i bankenes registre?
    - Å kartlegge hele leverandørkjeden vil ta lang tid da informasjon må innhentes i hvert ledd, sammen med at det kan være nødvendig å tilpasse kontrakter i alle ledd. Tas det høyde for at dette vil være et pågående arbeid etter at DORA trer i kraft?
12. Vil revisorer, regnskapsførere, eiendomsmeglere og inkassoforetak vil bli omfattet av det nye regelverket?

Mottatte spørsmål

13. Rapportering av hendelser
    a) For et konsern med flere finansielle enheter, vil en sentralisert enhet for innsending av hendelsesmeldinger og rapporter anses som outsourcing til en tredjepartsleverandør iht. 19(5) av DORA?
    b) Vurderer NO-FSA å utvikle og levere en mal for varsling av større IKT-relaterte hendelser?
    c) Relatert til innsending av varsling om større IKT-relaterte hendelser, hvilken kanal vil NO-FSA forvente at finansielle enheter bruker for varslingen?
    d) Er b) og c) ovenfor diskutert og ment på linje med de tre andre nordiske finanstilsynene?
14. Hvordan vil implementeringen av DORA forholde seg til NIS2-implementeringen i Norge?

FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY