FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DORA

7. april 2025

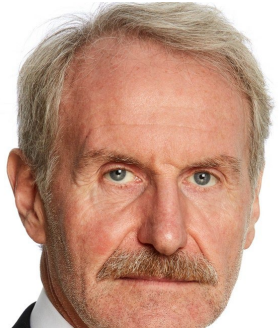
Tema

Litt overordnet om regelverket	Olav
Sentrale områder knyttet til etableringen av risikostyringssystem for IKT-virksomheten	Jarleif og Atle

Foredragsholderne

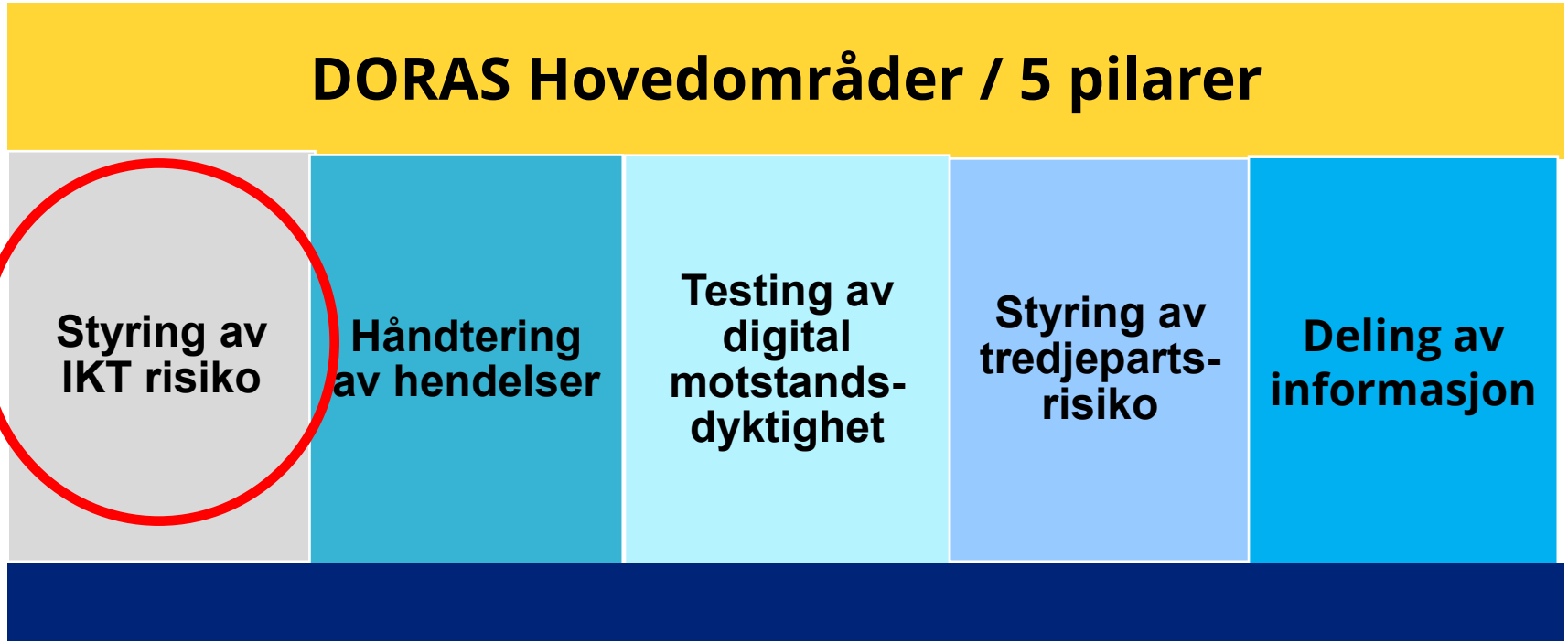
Jarleif Lødøen

Atle Dingsør



Olav Johannessen

DORA HOVEDOMRÅDER



Oversikt over RTS og ITS – Regelverk på nivå 2 (L2)

DORA-pillar	Referanse til DORA (L1)	Tilhørende RTS og ITS (DORA L2)
IKT-risikostyring (ICT Risk Management)	Kapittel II (Artiklene 5-16)	RTS on ICT Risk Management Framework and Simplified Framework (32024R1774)
		RTS on Policies for ICT Third-Party Service Providers (32024R1773)
		ITS on the Register of Information (32024R2956)
		RTS on Subcontracting ICT Services (Not yet assigned; under review)
Håndtering av hendelser (ICT-Related Incident Management and Reporting)	Kapittel III (Artiklene 17-20)	RTS on Classification of ICT-Related Incidents and Cyber Threats (32024R1772)
		RTS on Reporting of Major ICT-Related Incidents and Significant Cyber Threats (32025R0301)
		ITS on Reporting Templates for Major ICT-Related Incidents and Cyber Threats (32025R0302, assumed)
Testing av digital motstands-dyktighet (Digital Operational Resilience Testing)	Kapittel IV (Artiklene 24-27)	RTS on Threat-Led Penetration Testing (TLPT) (Not specified; likely published in 2025)
Styring av tredjeparts-risiko (ICT Third-Party Risk Management)	Kapittel V (Artiklene 28-44)	RTS on Criteria for Critical ICT Third-Party Service Providers (32024R1502)
		RTS on Harmonisation of Oversight Activities (32025R0420)
		RTS on Joint Examination Team (JET) Composition (Not specified; likely published in 2025)
		RTS on Subcontracting ICT Services (Not yet assigned; under review, also relevant here)
		ITS on the Register of Information (32024R2956, also relevant here)
Deling av informasjon Information Sharing	Kapittel VI (Artikkel 45)	No specific RTS or ITS mandated; pillar relies on voluntary arrangements under Article 45

Litt overordnet om regelverket knyttet til styring av IKT-risiko etter DORA

Regler om styring av IKT-risiko i DORA

Nivå 1-regelverk

DORA-forordningen (EU) 2022/2554

- Kapittel I, art. 5
- Kapittel II, art. 6-16

Nivå 2-regelverk

«RTS»

Delegert kommisjonsforordning (EU) 2024/1774 om spesifisering av rammeverket for styring av IKT-risiko, inkludert forenklet rammeverk for nærmere definerte (små) foretak

Art 6 (L1) – OVERSIKT – RTS-krav og mandat

DORA - RTS krav, og mandat	L1 - RTS-krav	L1 – RTS-Mandat
Artikkel 5: Styring og organisering		
Artikkel 6: Rammeverk for IKT-risikostyring	Art 6(5)	Art 15 (g)
Artikkel 7: IKT-systemer, -protokoller og -verktøyer		
Artikkel 8: Identifisering (**IDENTIFY**)		
Artikkel 9: Beskyttelse og forebygging (**PROTECT**)	Art 9(2)	Art 15 (a)
	Art 9(4) c)	Art 15 (b)
Artikkel 10: Påvisning (**DETECT**)	Art 10(1)	Art 15 (c)
	Art 10(1)	
Artikkel 11: Respons og gjenoppretting (**RESPOND**)	Art 11(1)	Art 15(d)
	Art 11(3)	Art 15(f)
	Art 11(6)	Art 15(e)
Artikkel 12: Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting (**RECOVER**)		
Artikkel 13: Læring og utvikling		
Artikkel 14: Kommunikasjon		
Artikkel 15: Ytterligere harmonisering av verktøyer, metoder, framgangsmåter og retningslinjer for IKT-risikostyring		
Artikkel 16: Forenklet rammeverk for IKT-risikostyring		

Eksempel på peking mellom nivå 1 og 2

DORA artikkel	Tekst	RTS	
Artikkel 8	1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.	Artikkel 4	2. The policy on management of ICT assets referred to in paragraph 1 shall: (a) prescribe the monitoring and management of the lifecycle of ICT assets identified and classified in accordance with Article 8(1) of Regulation (EU) 2022/2554;
		Artikkel 10	2. The vulnerability management procedures referred to in paragraph 1 shall: (b) ensure the performance of automated vulnerability scanning and assessments on ICT assets, whereby the frequency and scope of those activities shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset;
		Artikkel 11	2. The data and system security procedure referred to in paragraph 1 shall contain all of the following elements related to data and ICT system security, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554:

Eksempel på peking mellom nivå 1 og 2

DORA artikkel	Tekst	RTS	
Artikkel 10	2. The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	Artikkel 6	4. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 provisions for updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis. Those updates or changes shall ensure that the cryptographic technology remains resilient against cyber threats, as required by Article 10(2), point (a). Financial entities that are not able to update or change the cryptographic technology shall adopt mitigation and monitoring measures that ensure resilience against cyber threats
		Artikkel 23	5. Financial entities shall consider all of the following criteria to trigger the ICT-related incident detection and response processes referred to in Article 10(2) of Regulation (EU) 2022/2554:

Sentrale begreper i regelverket

«Management body» eller «ledelsesorgan»

«…bør tillegges styret og daglig leder i foretaket, i tråd med den alminnelige selskapsrettslige ansvarsfordelingen mellom disse organene i norsk rett.»

«…ansvaret for den operative virksomheten normalt ligger hos daglig leder, mens styret på sin side skal sørge for forsvarlig organisering og føre tilsyn med selskapets virksomhet.»

«Der det er usikkerhet om ansvarsfordelingen, påhviler det styret i det enkelte foretak å sørge for en avklaring om hva som er eller skal være styrets ansvar og hva som skal være ledelsens (daglig leders) ansvar.»

Hentet fra Prop. 54 LS (2024-2025) s. 28-29

Proporsjonalitet (artikkel 4)

Momenter:

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

IKT-risiko vs Cyberrisiko i DORA

IKT-risiko	Risiko knyttet til alle aspekter av nettverks- og informasjonssystemer, inkludert tekniske, operasjonelle og fysiske trusler, som kan kompromittere sikkerheten og påvirke driften.
Cyberrisiko	• Ikke eksplisitt definert • Utledes som en underkategori av IKT-risiko, spesifikt relatert til digitale trusler fra ondsinnede aktører og trusler i cyberspace.

Sanksjonering etter DORA – relevant for styring av IKT-risiko

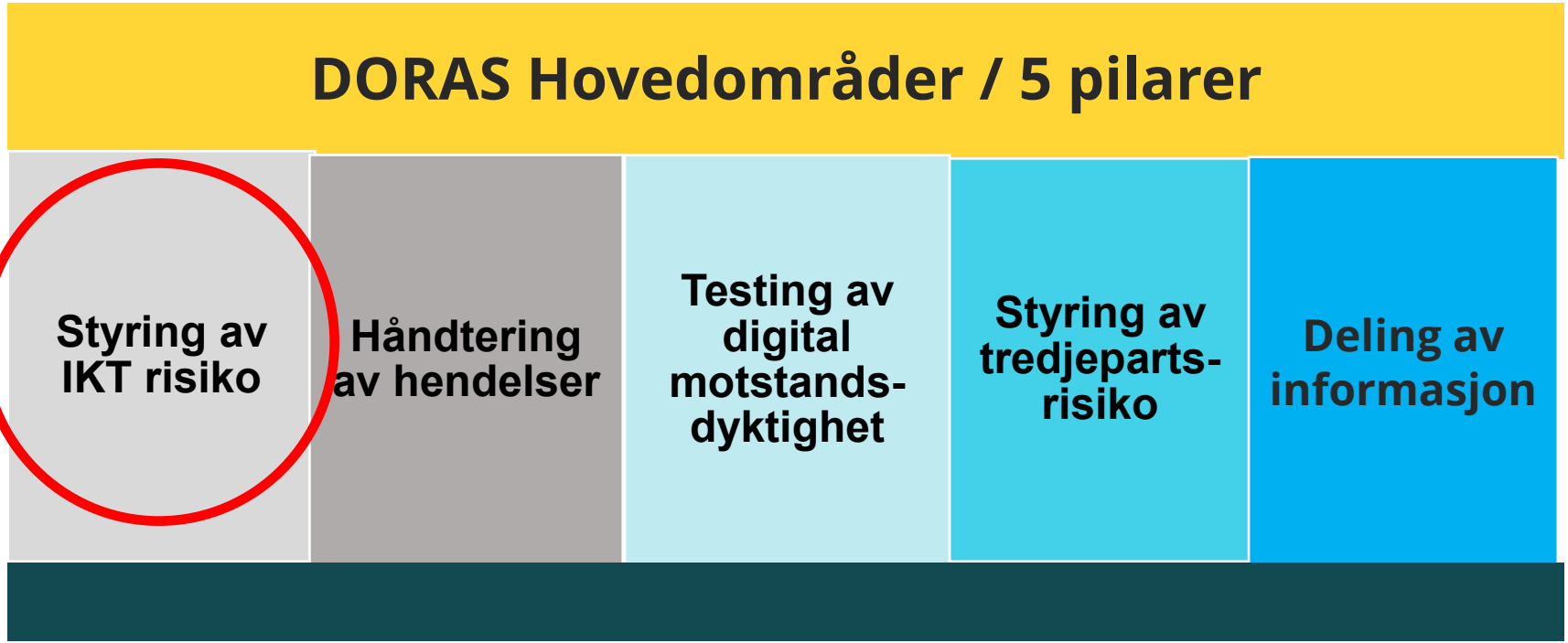
Finanstilsynet kan ilegge …… overtredelsesgebyr …… ved overtredelse av følgende bestemmelser i DORA-forordningen:

a. artikkel 5 om forvaltning og organisasjon,
b. artikkel 6 om rammeverk for IKT-risikostyring,
c. artikkel 8 om identifisering av IKT-relaterte funksjoner og avhengigheter,
d. artikkel 9 nr. 4 om retningslinjer for sikkerhet mv. som del av rammeverket for IKT-risikostyring, jf. artikkel 6,
e. artikkel 11 om respons og gjenoppretting,
f. artikkel 12 om retningslinjer og prosedyrer for sikkerhetskopiering og gjenoppretting,
g. artikkel 14 om planer for krisekommunikasjon,
h. artikkel 16 nr. 1 og 2 om forenklet rammeverk for IKT-risikostyring

Tilsvarende ved overtredelse av forskrifter som gjennomfører RTSer fastsatt etter DORA-forordningen artikkel 15 og artikkel 16 nr. 3

IKT-Risikostyring

DORA HOVEDOMRÅDER



DORA (L1), Kap. 2 - Rammeverk for styring av IKT risiko

- **Avsnitt I** omfatter dekker styring og organisering: (Artikkel 5 - Governance and Organisation)
  - Artikkel 5
    - Artikkel 5: Styring og organisering (Governance and organisation)
- **Avsnitt II** omfatter
  - Artikkel 6 – 14 – Detaljtemaer
    - Artikkel 6: Ramme for IKT-risikostyring (ICT Risk Management Framework)
    - Artikkel 7: IKT-systemer, -protokoller og -verktøyer (ICT Systems, Protocols and Tools)
    - Artikkel 8: Identifisering (Identification)
    - Artikkel 9: Beskyttelse og forebygging (Protection and Prevention)
    - Artikkel 10: Påvisning (Detection)
    - Artikkel 11: Respons og gjenoppretting (Response and Recovery)
    - Artikkel 12: Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting (Backup policies and procedures, restoration and recovery procedures and methods)
    - Artikkel 13: Læring og utvikling (Learning and Evolving)
    - Artikkel 14: Kommunikasjon (Communication)
  - Artikkel 15 og 16 – Utelates

NIST/DORA

Selv om det her vises til sammenhengen mellom NIST og DORA vil Finanstilsynet gjøre oppmerksom på at andre rammeverk er vel så relevante å se hen til i arbeidet med IKT-sikkerhet.

Prinsipper for informasjonssikkerhet

Integritet (Integrity)	Sikrer at data er nøyaktige og ikke har blitt endret eller manipulert.
Konfidensialitet (Confidentiality)	Beskytter data mot uautorisert tilgang og sikrer at kun autoriserte personer kan se sensitiv informasjon.
Tilgjengelighet (Availability)	Sikrer at data og systemer er tilgjengelige når de trengs, og at de fungerer som forventet.
Autentisitet (Authenticity)	Bekrefter at data og brukere er ekte og kommer fra pålitelige kilder.
Ikke-fornektelse (Non-repudiation)	Gir bevis på at en handling eller transaksjon har funnet sted, og hindrer at noen kan benekte at de har utført den.

Redusere sikkerhetsrisiko og sikre digital operasjonell motstandskraft (NIST CSF*/DORA)

*) **NIST CSF** står for **N**ational **I**nstitute of **S**tandards and **T**echnology **C**ybersecurity **F**ramework

IDENTIFY	Utvikle kunnskap og forståelse av organisasjonens cybersikkerhetsrisiko til systemer, mennesker, eiendeler, data og kapabiliteter.
PROTECT	Implementere beskyttelsestiltak som sikrer leveransen av kritiske infrastrukturtjenester.
DETECT	Etablere mekanismer for å identifisere cybersikkerhetshendelser.
RESPOND	Utvikle og implementere planer for å håndtere cybersikkerhetshendelser.
RECOVER	Implementere tiltak som kan sikre gjenoppretting av kapabiliteter eller tjenester som kan bli påvirket av cybersikkerhetshendelse.

- Prinsippene fra informasjonssikkerhet, som integritet, konfidensialitet, tilgjengelighet, autentisitet og ikke-fornektelse, er viktige dimensjoner når man skal vurdere kjernefunksjonene som er basis i DORA/NIST Cybersecurity Framework: IDENTIFY, PROTECT, DETECT, RESPOND og RECOVER.

- Grupperingen i disse kjernefunksjonene hjelper organisasjoner med å få fokus på å beskytte informasjon mot uautorisert tilgang, manipulering og avbrudd. Den gir også en god ramme for hvordan man skal håndtere cybersikkerhetsrisikoer gjennom livssyklusen til informasjonssystemer.

NIST (DORA) – IDENTIFY og PROTECT

IDENTIFY

Integritet	Identifisere og kartlegge risikoer som kan påvirke integriteten til data og systemer.
Konfidensialitet	Identifisere sensitive data og systemer som må beskyttes mot uautorisert tilgang.
Tilgjengelighet	Kartlegge kritiske systemer og ressurser som må være tilgjengelige for å opprettholdvirksomhetens drift.
Autentisitet	Identifisere mekanismer for å verifisere opprinnelsen til data og brukere.
Ikke-fornektelse	Identifisere tiltak for å sikre at handlinger og transaksjoner kan bevises og ikke kan benektes.

PROTECT

Integritet	Implementere sikkerhetstiltak som beskytter data mot uautorisert endring.
Konfidensialitet	Implementere tilgangskontroller og kryptering for å beskytte sensitive data.
Tilgjengelighet	Sikre at systemer og data er tilgjengelige når de trengs.
Autentisitet	Implementere autentiseringsmekanismer for å verifisere brukere og data.
Ikke-fornektelse	Implementere digitale signaturer og kryptografiske nøkler for å sikre at handlinger kan bevises.

NIST (DORA) – DETECT og RESPOND

DETECT

Integritet	Overvåke systemer for å oppdage uautorisert endring av data.
Konfidensialitet	Overvåke systemer for å oppdage uautorisert tilgang til sensitive data.
Tilgjengelighet	Overvåke systemer for å oppdage avbrudd eller nedetid.
Autentisitet	Overvåke systemer for å oppdage forsøk på etterligning eller identitetstyveri.
Ikke-fornektelse	Overvåke systemer for å oppdage forsøk på å benekte handlinger.

RESPOND

Integritet	Utvikle og implementere tiltak for å gjenopprette integriteten til data etter en hendelse.
Konfidensialitet	Utvikle og implementere tiltak for å beskytte sensitive data etter en hendelse.
Tilgjengelighet	Utvikle og implementere tiltak for å gjenopprette tilgjengeligheten til systemer og data etter en hendelse.
Autentisitet	Utvikle og implementere tiltak for å verifisere opprinnelsen til data etter en hendelse.
Ikke-fornektelse	Utvikle og implementere tiltak for å sikre at handlinger kan bevises etter en hendelse.

NIST (DORA) – RECOVER

RECOVER

Integritet	Gjenopprette integriteten til data og systemer etter en hendelse.
Konfidensialitet	Gjenopprette beskyttelsen av sensitive data etter en hendelse.
Tilgjengelighet	Gjenopprette tilgjengeligheten til systemer og data etter en hendelse.
Autentisitet	Gjenopprette mekanismer for å verifisere opprinnelsen til data etter en hendelse.
Ikke-fornektelse	Gjenopprette mekanismer for å sikre at handlinger kan bevises etter en hendelse.

Kort om DORA (EU) 2022/2554 (L1) dette webinaret

FRA DORA-lovgivningen (L1) - KAPITTEL II: IKT-RISIKOSTYRING		Omhandles nå
Artikkel 5	Styring og organisering (Governance and organisation)	x
Artikkel 6	Ramme for IKT-risikostyring (ICT risk management framework)	x
Artikkel 7	IKT-systemer, -protokoller og -verktøyer (ICT systems, protocols and tools)	
Artikkel 8	Identifisering (**Identification**)	x
Artikkel 9	Beskyttelse og forebygging (**Protection and prevention**)	x
Artikkel 10	Påvisning (**Detection**)	x
Artikkel 11	Respons og gjenoppretting (**Response and recovery**)	x
Artikkel 12	Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting (Backup policies and procedures, restoration and recovery procedures and methods)	(x)
Artikkel 13	Læring og utvikling (Learning and evolving)	
Artikkel 14	Kommunikasjon (Communication)	
Artikkel 15	Ytterligere harmonisering av verktøyer, metoder, framgangsmåter og retningslinjer for IKT-risikostyring (Further harmonisation of ICT risk management tools, methods, processes and policies)	
Artikkel 16	Forenklet rammeverk for IKT-risikostyring (Simplified ICT risk management framework)	X

NIST (DORA) – Målsetninger for hovedfunksjonene

1. Identify (Identifisere)	
Mål	Forstå organisasjonens cybersikkerhetsrisiko ved å identifisere kritiske ressurser, systemer, data og potensielle trusler.
Aktiviteter	Kartlegging av eiendeler (hardware, software, data), vurdering av risiko, etablering av styringsstrukturer og forståelse av forretningskonteksten.
Eksempel	Finne ut hvilke systemer som er mest kritiske for driften og hvilke trusler som kan påvirke dem.
2. Protect (Beskytte)	
Mål	Implementere tiltak for å beskytte organisasjonens eiendeler mot cybertrusler.
Aktiviteter	Tilgangskontroll, opplæring av ansatte, bruk av kryptering, vedlikehold av systemer og bruk av sikkerhetsteknologier.
Eksempel	Sette opp brannmurer og trene ansatte i å unngå phishing-angrep.
3. Detect (Oppdage)	
Mål	Identifisere cyberhendelser raskt når de oppstår.
Aktiviteter	Overvåking av systemer, logging av aktiviteter, bruk av deteksjonssystemer og varsling ved unormale hendelser.
Eksempel	Bruke et intrusjonsdeteksjonssystem (IDS) for å oppdage uautorisert tilgang.
4. Respond (Reagere)	
Mål	Håndtere og begrense skade når en cyberhendelse har blitt oppdaget.
Aktiviteter	Utarbeide responsplaner, kommunisere med interessenter, analysere hendelsen og iverksette tiltak for å stoppe spredning.
Eksempel	Isolere et infisert nettverk og informere berørte parter om et datainnbrudd.
5. Recover (Gjenopprette)	
Mål	Gjenopprette normale operasjoner og styrke motstandskraft etter en hendelse.
Aktiviteter	Gjenoppretting av systemer og data (f.eks. fra sikkerhetskopier), evaluering av hendelsen og forbedring av prosesser.
Eksempel	Gjenopprette tapte filer fra en backup og oppdatere sikkerhetspolicyer basert på erfaringer.

OM DORA (L1) Artikkel 8 – 11 og kobling til NIST

- **NIST har fastsatt kjernefunksjonene slik**

IDENTIFY	Utvikle kunnskap og forståelse av organisasjonens cybersikkerhetsrisiko til systemer, mennesker, eiendeler, data og kapabiliteter.
PROTECT	Implementere beskyttelsestiltak som sikrer leveransen av kritiske infrastrukturtjenester.
DETECT	Etablere mekanismer for å identifisere cybersikkerhetshendelser.
RESPOND	Utvikle og implementere planer for å håndtere cybersikkerhetshendelser.
RECOVER	Implementere tiltak som kan sikre gjenoppretting av kapabiliteter eller tjenester som kan bli påvirket av cybersikkerhetshendelse.

- **Slik er disse gruppert i DORA:**

Identifisering (**IDENTIFICATION**)	**Artikkel 8**
Beskyttelse og forebygging (**PROTECTION AND PREVENTION**)	**Artikkel 9**
Påvisning (**DETECTION**)	**Artikkel 10**
Respons og gjenoppretting (**RESPONSE AND RECOVERY**)	**Artikkel 11**

DORA-Lovgivningen (L1)

Kort om DORA (EU) 2022/2554 (L1) dette webinaret

FRA DORA (Lovgivningen) - KAPITTEL II: IKT-RISIKOSTYRING		Omhandles nå
Artikkel 5	Styring og organisering (Governance and organisation)	x
Artikkel 6	Ramme for IKT-risikostyring (ICT risk management framework)	x
Artikkel 7	IKT-systemer, -protokoller og -verktøyer (ICT systems, protocols and tools)	
Artikkel 8	Identifisering (**Identification**)	x
Artikkel 9	Beskyttelse og forebygging (**Protection and prevention**)	x
Artikkel 10	Påvisning (**Detection**)	x
Artikkel 11	Respons og gjenoppretting (**Response and recovery**)	x
Artikkel 12	Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting (Backup policies and procedures, restoration and recovery procedures and methods)	(x)
Artikkel 13	Læring og utvikling (Learning and evolving)	
Artikkel 14	Kommunikasjon (Communication)	
Artikkel 15	Ytterligere harmonisering av verktøyer, metoder, framgangsmåter og retningslinjer for IKT-risikostyring (Further harmonisation of ICT risk management tools, methods, processes and policies)	
Artikkel 16	Forenklet rammeverk for IKT-risikostyring (Simplified ICT risk management framework)	X

Kommer **kort inn om de gulmarkerte** fra DORA-lovigningen (L1) før vi går inn i RTS en for IKT-risikostyring

Art 5 (L1): Styring og organisering (styre/ledelse)

Etablere virksomhetsstyring med et kontrollrammeverk som sikrer effektiv og forsvarlig styring av IKT-risiko

Styre og daglig leder skal føre tilsyn med, og er ansvarlig for, IKT-risikostyringen

Definere klare roller og ansvarsområder

Definere og godkjenne strategi for digital operasjonell motstandskraft, samt fastsette foretakets toleransenivå for IKT-risiko.

Kontrollere og vurdere retningslinjene for beredskap og kontinuitet, samt IKT-respons- og -gjenopprettingsplaner.

Vurdere (interne) revisjonsplaner for IKT, samt beslutte hvilke IKT-revisjoner som skal gjennomføres.

Art 6 (L1)- IKT risikostyringsrammeverk

Helhetlig IKT-risikostyringsrammeverk	Sikre rask, effektiv og grundig håndtering av IKT-risiko.
	Skal støtte opp om digital operasjonell motstandskraft.
Beskyttelse av IKT-ressurser	Strategier, policyer og verktøy for å beskytte informasjonsressurser (programvare, maskinvare, servere, lokaler, datasentre, etc.).
	Forhindre skade, uautorisert tilgang og misbruk.
Minimere konsekvenser av IKT-risiko	Innføringen av passende risikoreduserende strategier og verktøy.
	Skal kunne gi oppdatert informasjon om IKT-risiko til myndighetene.
Uavhengig oppfølging	Uavhengig kontrollfunksjon skal styre og føre tilsyn med IKT-risiko.
	Skille mellom av IKT-risikostyring, kontroll og revisjonsfunksjoner.
Årlig gjennomgang og kontinuerlig forbedring	Rammeverk som blir gjennomgått minst årlig eller etter betydelige IKT-hendelser.
	Rapport som kan sendes til myndighetene på forespørsel.
Digital operasjonell motstandsstrategi	Støtter forretningsmål, risikotoleranse og påvirkningstoleranse.
	Setter klare mål for informasjonssikkerhet og testmekanismer.
	Kommunikasjonsstrategi for IKT-relaterte hendelser.
Strategi for tredjeparts tjenesteleverandører	Helhetlig IKT-multileverandørstrategi som viser avhengigheter og forklarer sammensetningen av tredjepartsleverandører av IKT-tjenester.
	Må sikre etterlevelsen for tjenestekjøp fra tredjeparter, der ansvaret for de utkontrakterte tjenestene uansett er hos foretaket.

RTS Mandat 15 (g): Nærmere innhold og format for rapporten i artikkel 6 nr. 5. - Artikkel 27, i RTS for IKT-Risikostyringsrammeverket.

Art 8 (L1): Identifisering (Identification)

Klassifisere og dokumentere IKT-eiendeler	Identifisere, klassifisere og dokumentere alle IKT-støttede forretningsfunksjoner, roller og ansvar, samt informasjons- og IKT-ressurser forbundet med disse.
	Vurdere hvorvidt klassifiseringen og relevant dokumentasjon er tilstrekkelig minst årlig.
Kontinuerlig risikoidentifisering	Finansielle enheter skal kontinuerlig identifisere alle kilder til IKT-risiko og vurdere cybertrusler, IKT-sårbarheter og eksterne avhengigheter
	Regelmessig gjennomgang av risikoscenarier, minst årlig.
Risikovurdering ved større endringer	Finansielle enheter skal utføre risikovurdering ved større endringer i nettverk og informasjonssystemer.
	Risikovurdering av endringen før gjennomføring, og risikovurdering av situasjonen som vil være etter endringen er utført.
Identifikasjon av IKT-ressurser	Identifisere alle IKT-ressurser, inkludert eksterne datasenter, nettverksressurser og kritisk hardware, og kartlegge de som anses som kritiske
	Dokumentere enhetenes konfigurasjon og avhengigheter.
Avhengighet av tredjepartsleverandører	Finansielle enheter må dokumentere alle prosesser og koblinger til IKT-tredjepartsleverandører som støtter kritiske funksjoner.
Vedlikehold av utstyrsoversikter	Sikre at oversikter over IKT-eiendeler er oppdatert.
Risikovurdering av eldre systemer	Finansielle enheter skal regelmessig gjennomføre risikoanalyser av alle eldre IKT-systemer, spesielt før og etter integrasjon av ny teknologi.

Art 8 (L1): Om klassifisering i DORA

Uten korrekt klassifisering vil foretakene kunne slite med å vurdere risiko, beskytte driften og oppfylle DORA-kravene:

- **Hva skal klassifiseres – DORA (L1), Artikkel 8 (1)**
  - **Informasjonsressurser:** en samling av opplysninger, både materielle og immaterielle, som det er verdt å beskytte. Eksempel: Kundedata, transaksjonsdetaljer eller immaterielle rettigheter
  - **IKT-ressurser:** programvare- eller maskinvareressurs i nettverks- og informasjonssystemene som brukes av den finansielle enheten. Eksempel: Servere, applikasjoner eller skytjenester

- **Klassifiseringene inngår i oversikter over:**
  - **Kritiske eller viktige funksjoner**: Ressurser klassifiseres basert på om de støtter funksjoner hvor avbrudd ville svekke virksomhetens ytelse, tjenesteleveranse eller regulatorisk etterlevelse betydelig.
  - **IKT- eller informasjonsressurser:** Ressurser vurderes ut fra eksponering for IKT-risikoer, som cybertrusler og sårbarheter.
  - **Avhengighetskartlegging:** Ressurser vurderes utfra hvor kritiske de er i forhold til avhengigheter og sammenhenger, både internt og med tredjeparter for å ha kontroll med avbruddsituasjoner.

Art 9 (L1): Beskyttelse og forebygging (Protection and Prevention)

Kontinuerlig overvåking og risiko minimering	Overvåke og kontroller IKT-systemer for å ha kontroll med sikkerhet og funksjonalitet.
	organisere mottiltak i form av sikkerhetsverktøy, policyer og prosedyrer for å minimere IKT-risiko.
Sikring av IKT-systemenes digital motstandsevne	Implementer sikkerhetspolicyer og verktøy for å opprettholde motstandskraft, kontinuitet og tilgjengelighet.
	Sikre dataens integritet, autentisitet, konfidensialitet og tilgjengelighet.
Sikre IKT-løsninger og Prosesser	Sikre dataoverføring og forhindre uautorisert tilgang eller datatap.
	Beskytt mot tekniske feil, menneskelige feil og dårlig databehandling.
Nøkkeltiltak for IKT-beskyttelse	Informasjonssikkerhetspolicy – Definerer regler for beskyttelse av data og eiendeler.
	Nettverk & Infrastruktur Sikkerhet – Automatiserte mekanismer for å isolere cybertrusler.
	Tilgangskontrollpolicyer – Begrens tilgang til autoriserte funksjoner.
	Autentisering & Kryptering – Implementer sterk autentisering og kryptografisk beskyttelse.
	Endringsadministrasjonsprosedyrer – Sørge for sikre programvare-, maskinvare- og systemoppdateringer.
	Patch-administrasjon – Vedlikehold policyer for raske oppdateringer og sikkerhetspatching.
Sikker Nettverksarkitektur	Design infrastruktur for å segmentere eller isolere berørte områder under cyberhendelser.
	Implementer streng endringsadministrasjon godkjent av ledelsen.

Art 10 (L1): Påvisning (Detection)

- Etablere og regelmessig teste mekanismer for raskt å oppdage uvanlige aktiviteter, inkludert ytelsesproblemer i IKT-nettverket og IKT-relaterte hendelser, og identifisere potensielle kritiske enkeltpunktsfeil (single point of failure)

- Definer varslingsgrenser og kriterier for å utløse og starte IKT-relaterte hendelsesresponsprosesser, inkludert automatiske varslingsmekanismer til relevant personale som er ansvarlig for IKT-relaterte hendelsesrespons

- Alloker tilstrekkelige ressurser og kapasiteter for å overvåke brukeraktivitet, forekomsten av IKT-anomalier og IKT-relaterte hendelser, spesielt cyberangrep.

- Leverandører av datarapporteringstjenester skal i tillegg has systemer som effektivt sjekke handelsrapporter for fullstendighet, identifisere utelatelser og åpenbare feil, og be om ny overføring av disse rapportene.

Art 11: Respons og gjenoppretting (Response and Recovery)

Mål: Sikre kontinuitet i kritiske funksjoner, raskt respondere på og løse IKT-relaterte hendelser, og minimere skade

Nøkkelkomponenter i respons og gjenopprettingen	Omfattende IKT-forretningskontinuitetspolicy
	Dedikerte ordninger, planer, prosedyrer, og mekanismer
	Krisehåndteringsfunksjon (for ikke-mikroforetak)
	Kommunikasjon og krisehåndteringsplaner
Krav	Gjennomføre driftskonsekvensanalyse (BIA) for å vurdere potensiell effekt av alvorlige forretningsforstyrrelser
	Implementere og vedlikeholde IKT-forretningskontinuitetsplaner
	Teste IKT-forretningskontinuitetsplaner og respons- og gjenopprettingsplaner minst årlig, der det foretas endringer basert på testresultater (scenarioer skal testes)
	Dokumentere aktiviteter under avvikshendelser (lett tilgjengelige) når planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting aktiveres
Rapportering og intern revisjon	På anmodning fra myndighetene rapportere estimat på aggregerte årlige kostnader og tap forårsaket av store IKT-relaterte hendelser (for ikke-mikroforetak)
	Gi kopier av IKT-forretningskontinuitetstestresultater til kompetente myndigheter (for **verdipapirsentraler**)
	Uavhengige interne revisjonsgjennomganger av IKT-respons- og gjenopprettingsplaner (for ikke-mikroforetak)

RTS-Detaljer

Delegert kommisjonsforordning (EU) 2024/1774

Art 1 - Overall risk profile and complexity

Når IKT-sikkerhetspolicyer, prosedyrer, protokoller og verktøy utvikles og implementeres, skal det tas hensyn til foretakets størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift inkludert forhold knyttet til

- kryptering og kryptografi
- IKT-driftssikkerhet
- nettverkssikkerhet

Art 2 - General elements of ICT security policies, procedures, protocols, and tools

- (1) Foretaket må sikre at deres IKT-sikkerhetspolicyer, informasjonssikkerhet og tilhørende prosedyrer, protokoller og verktøy er integrert i IKT-risikostyringsrammeverket (jf. DORA (L1) - Article 9(2)).
- (2) IKT-sikkerhetspolicyene må være i samsvar med finansinstitusjonens informasjonssikkerhetsmål inkludert strategien for digital operasjonelle motstandskraft (jf. DORA (L1) - in Art 6(8)).

  IKT-sikkerhetspolicyen må angi konsekvenser for ansatte ved manglende overholdelse av IKT-sikkerhetspolicyene der dette ikke er regulert i andre policyer, inneholde en liste over dokumentasjon som må vedlikeholdes, og fastsette ansvarsdelingen ift. 3LOD eller annet for å unngå interessekonflikter.

Art 3 - ICT risk management

Foretaket må utvikle, dokumentere og implementere retningslinjer og prosedyrer for IKT-risikostyring som må omfatte

- godkjenning av risikotoleransenivået for IKT-risiko
- prosedyre og metodikk for å gjennomføre IKT-risikovurdering
- prosedyre for å identifisere og dokumentere tiltak for å håndtere IKT-risiko, inkludert å bestemme nødvendige risikoreduserende tiltak.
- prosedyrer for å håndtere restrisiko (etter implementering av risikoreduserende tiltak)
- sikre at endringer i virksomhetens strategi og i den digitale operasjonelle strategien for digital motsandskraft hensyntas.

Art 4 og Art 5 – IKT-eiendelsstyringspolicy og -prosedyre

Ved å ha en grundig og dokumentert oversikt over alle IKT eiendeler kan man bedre vurdere risiko, sikre kontinuitet i driften, og beskytte sensitive data mot eksterne trusler.

Artikkel 4: IKT eiendelstyringspolicy

- mål om å overvåke og administrere livssyklusen til identifiserte og klassifiserte IKT eiendeler (jf. DORA-loven Art 8(1)
- etablere oversikter over utstyr med unike identifikatorer, plassering, klassifisering, eiere, støttede forretningsfunksjoner, kontinuitetskrav, eksponering mot eksterne nettverk, sammenkoblinger, utløpsdatoer .

Artikkel 5: IKT eiendelsstyringsprosedyre

- utvikle, dokumentere og implementere klare retningslinjer og prosedyrer for håndtere IKT-aktiva
- spesifisere kriterier for å vurdere kritikaliteten til informasjon og IKT-aktiva som støtter forretningsfunksjoner

Art 8 - Policies and procedures for ICT operations

Som del av IKT-sikkerhetspolicyen, prosedyrer, protokoller og verktøy nevnt i DORA-Loven, artikkel 9(2) skal foretaket utvikle, dokumentere og implementere retningslinjer og prosedyrer for å administrere IKT-driften.

Policyene og prosedyrene for IKT-operasjoner skal inneholde følgende:

- Beskrivelse av IKT-ressurser

- Kontroll og overvåking av IKT-systemer

- Feilhåndtering knyttet til IKT-systemer

Project and change management (Art 15, 16 og 17) - (1)

Disse **tre artiklene** beskriver detaljene rundt risikostyring knyttet til IKT-systemer, inkludert prosjektledelse, systemanskaffelse, utvikling og endringshåndtering.

Den dekker viktige aspekter som testing, implementering, sikkerhet, og nødvendige tiltak for å sikre at endringer ikke kompromitterer systemets integritet.

Artikkel 15: IKT prosjektledelse

Foretaket må utvikle, dokumentere og implementere en IKT prosjektledelsespolicy som spesifiserer elementer for effektiv håndtering av IKT-prosjekter relatert til anskaffelse, vedlikehold og utvikling av IKT-systemer.

Project and change management (Art 15, 16 og 17) - (2)

Artikkel 16: IKT systemer anskaffelse, utvikling og vedlikehold

Foretaket skal utvikle, dokumentere og implementere en policy som styrer anskaffelse, utvikling og vedlikehold av IKT-systemer. Denne skal inneholde

- En metodikk for anskaffelse, utvikling og vedlikehold av IKT-systemer
- Krav om å innhente nærmere bestemte spesifikasjoner
- Kravene ved anskaffelse, utvikling og vedlikehold av IKT-systemer, med særlig fokus på IKT-sikkerhetskrav og godkjenning fra relevante forretningsfunksjon/systemeier
- Spesifisere tiltak for å redusere risiko for utilsiktet endring/bevisst manipulering av IKT-systemene
- Spesifikke krav til testing
- Spesielle krav til «Central securities depositories» (Verdipapirsentraler) - krav til hvem som skal delta design og testing

Project and change management (Art 15, 16 og 17) - (3)

Artikkel 17: IKT endringshåndtering

Foretaket må

- fastsette detaljerte prosedyrer for å sikre at alle endringer i programvare, maskinvare, fastvare/firmware, systemer og sikkerhetsparametere blir nøye vurdert og godkjent.
- I denne sammenheng er det viktig å
    - verifisere at IKT-sikkerhetskravene er oppfylt,
    - ha uavhengige funksjoner for godkjenning av endringer
    - klare roller og ansvar for spesifikasjon, planlegging, testing og implementering av endringer.
    - dokumentasjon og kommunikasjon av endringsdetaljer, inkludert nødprosedyrer og fall-back-løsninger, er også viktige elementer for å sikre en kontrollert og sikker overgang.
    - Spesifikke krav for «central counterparties» (Sentrale motparter) og «central securities depositories» (Verdipapirsentraler) om å sende IKT-systemene for «stress-testing», jf. Art 17(2)
-

Art 18 - Physical and environmental security

En gjennomtenkt fysisk og miljømessig sikkerhetspolitikk er avgjørende for å beskytte en finansinstitusjons data, IKT-ressurser og informasjon mot potensielle trusler, der det tas hensyn til foretakets risiko og klassifiseringen av IKT-ressurser.

Politikken skal inkludere

- referanse til policy for tilgangsstyring
- beskyttelsestiltak mot angrep, ulykker og miljøtrusler for enhetens lokaler, datasentre og sensitive områder hvor IKT-ressurser og informasjonsressurser befinner seg.
- tiltak for å sikre tilgjengeligheten, autentisiteten, integriteten og konfidensialiteten til disse ressursene
- sikre IKT-eiendelene både innenfor og utenfor foretakets lokaler
- sikre at fysiske tilgangskontroller fungerer

CHAPTER II: HR policy and access control (Art 19) (1)

DORA fremhever viktigheten av fysisk og miljømessig sikkerhet, samt identitets- og tilgangsstyring, som essensielle aspekter for å beskytte IKT-ressurser og forhindre uautorisert tilgang og trusler.

Artikkel 19: Human resources policy

Artikkelen understreker viktigheten av å blant annet inkludere følgende IKT-sikkerhetsrelatert elementer i foretakets **HR-policy**:

- Identifisere og tildele spesifikke ansvarsområder for IKT-sikkerhet
- Egne ansatte og ansatte hos tredjeparter skal være informert om og følge selskapets IKT-sikkerhetspolicyer og -rutiner
- Identitetsstyring skal sikre unik identifikasjon og autentisering av personer og systemer som får tilgang til informasjon
- Det skal finnes prosedyrene som omfatter livssyklushåndtering av identiteter og kontoer, inkludert opprettelse, endring, gjennomgang, oppdatering, midlertidig deaktivering og avslutning.
- Alle identitetsoppdrag skal registreres og arkiveres.
- Det skal finnes prosedyrer for rapportering av avvikende oppførsel
- Ansatte må levere tilbake alle IKT-ressurser ved avslutning av arbeidsforholdet.

Human resources policy and access control (Art 20) (2)

Artikkel 20: Identity management

Etablere, dokumentere og implementere **identitetsstyringspolicyer og -prosedyrer** som sikrer unik identifisering og autentisering av personer og systemer som får tilgang til foretakets informasjon, der kravene i artikkel 21 om «Access Control» ivaretas.

Dette inkluderer policyer og prosedyrer for livssyklusstyring av identiteter og kontoer, med etablering, endring, gjennomgang og deaktivering av kontoer. Det legges vekt på å føre oversikt over alle identiteter og bruke automatiserte løsninger der det er mulig, og at oversikter ivaretas også etter omorganiseringer.

Human resources policy and access control (Art 21) (3)

Artikkel 21: Access control

Artikkelen omhandler utvikling, dokumentasjon og implementere en policy for administrasjon av tilgangsrettigheter. Dette inkluderer tildeling av tilganger basert på prinsipper som

- "need-to-know" og "least privilege«
- separasjon av plikter (separation of duties) for å forhindre uberettiget tilgang til kritiske data

Ande momenter er

- at bruken av generiske og delte brukerkontoer skal reduseres til et minimum slik at man sikrer at brukere er identifiserbare for utførte handlinger
- Autentiseringsmetoder i tråd med klassifiseringen, jf. DORA-lovgivingen
- Detaljert beskrevne Fysisk aksesskontroller som er detaljert beskrevet

CHAPT III: ICT-related incident detection and response (1)

Artikkel 22 og 23 har som formål å etablere, dokumentere og implementere en policy for håndtering av IKT-relaterte hendelser hos finansielle enheter.

- Artikkel 22 fokuserer på å opprette mekanismer for å oppdage, overvåke og håndtere unormale aktiviteter og cybertrusler.
- Artikkel 23 utdyper hvordan finansielle enheter skal identifisere, loggføre og analysere IKT-relaterte hendelser og unormale aktiviteter for å sikre dataintegritet og tilgjengelighet samt beskytte mot uautorisert tilgang og manipulering.

Article 22: ICT-related incident management policy

Foretaket skal utvikle, dokumentere og implementere en IKT-relatert hendelsespolicy der man

- dokumenterer prosessen for håndtering av IKT-relaterte hendelser som nevnt i Artikkel 17, «Prosess for håndtering av IKT-relaterte hendelser»
- etablere oversikt over relevante interne funksjoner og eksterne interessenter som er direkte involvert i drift knyttet til IKT-sikkerhet
- etablere, implementere og operere tekniske, organisatoriske og operasjonelle mekanismer for å støtte prosessen for håndtering av IKT-relaterte hendelser, inkludert mekanismer for rask oppdagelse av unormale aktiviteter og atferd
- fastsetter prinsippene for lagring av dokumentasjon knyttet til IKT-relaterte hendelser
- fastsetter og implementerer mekanismer for å analysere større eller gjentakende hendelser

CHAPT III: ICT-related incident detection and response (2)

Article 23: Anomalous activities detection and criteria for ICT-related incidents detection and response

→ Oppdagelse av avvikende aktiviteter og kriterier for oppdagelse og håndtering av IKT-relaterte hendelser

- Finansielle enheter skal fastsette klare roller og ansvar for å effektivt oppdage og håndtere IKT-relaterte hendelser og avvikende aktiviteter
- Mekanismen for rask oppdagelse av avvikende aktiviteter, inkludert IKT-nettverksytelsesproblemer og IKT-relaterte hendelser skal gjøre det mulig for finansielle enheter å:
    - samle, overvåke og analysere tilgjengelig informasjon
    - identifisere avvikende aktiviteter og atferd, og implementere verktøy som kan generere varsler for dette
    - kunne prioritere varslene for å håndter hendelser innen forventet løsningstid
    - registrere, analysere og evaluere all relevant informasjon om alle avvikende aktiviteter og atferd automatisk eller manuelt
    - ivareta beskyttelse av registreringer av avvikende aktiviteter mot manipulering og uautorisert tilgang
    - ha tilstrekkelig informasjon for å logge relevant informasjon tidspunkt for når avvik oppstod, når avvik ble oppdaget og typen avvik
    - å identifisere, registrere og håndtere IKT-hendelser basert på deres potensielle påvirkning på systemenes sikkerhet og integritet

CHAPTER IV: ICT business continuity management (1)

Disse tre artiklene har til hensikt å etablere retningslinjer og prosedyrer for å sikre forretningskontinuitet og respons på IKT-relaterte nødsituasjoner i foetaket. Artiklene dekker temaer som utvikling, testing og gjennomgang av IKT-retningslinjer for forretningskontinuitet, samt krav til respons- og gjenopprettingsplaner.

Artikkel 24 Components of the ICT business continuity policy:
Denne artikkelen beskriver komponentene i en IKT-forretningskontinuitetspolitikk, inkludert mål, omfang, tidsramme, og aktiverings- og deaktiveringskriterier. Den dekker også styringsstruktur, tilpasning av IKT-planer til overordnede forretningsplaner, og krav til testing og gjennomgang.

Artikkel 25 Testing of the ICT business continuity plans:
Denne artikkelen fokuserer på testing av IKT-forretningskontinuitetsplaner. Den beskriver kravene til testscenarier, inkludert simulering av potensielle forstyrrelser og switchover-scenarioer. Artikelen inneholder også krav til dokumentasjon og håndtering av eventuelle mangler som identifiseres under testing.

Artikkel 26 ICT response and recovery plans:
Denne artikkelen omhandler utviklingen av IT-respons- og gjenopprettingsplaner. Den beskriver kravene til disse planene, inkludert spesifikasjon av aktiverings- og deaktiveringsbetingelser, kortsiktige og langsiktige gjenopprettingsalternativer, og identifisering av relevante scenarier for alvorlige forretningsforstyrrelser.

CHAPTER IV: ICT business continuity management (2)

Artikkel 24 Components of the ICT business continuity policy:

Denne artikkelen beskriver komponentene i en IKT-forretningskontinuitetspolitikk, inkludert mål, omfang, tidsramme, og aktiverings- og deaktiveringskriterier. Den dekker også styringsstruktur, tilpasning av IKT-planer til overordnede forretningsplaner, og krav til testing og gjennomgang.

IKT-forretningskontinuitetspolitikken skal inneholde en **beskrivelse** av:

- målene for IKT-forretningskontinuitetspolitikken, inkludert sammenhengen mellom IKT og generell forretningskontinuitet, med hensyn til resultatene fra virksomhetspåvirkningsanalysen (BIA);
- omfanget av IKT-forretningskontinuitetsarrangementer, planer, prosedyrer og mekanismer, inkludert begrensninger og ekskluderinger;
- tidsrammen som skal dekkes av IKT-forretningskontinuitetsarrangementer, planer, prosedyrer og mekanismer;
- kriteriene for å aktivere og deaktivere IKT-forretningskontinuitetsplaner, IKT-respons- og gjenopprettingsplaner og krisekommunikasjonsplaner;

CHAPTER IV: ICT business continuity management (4)

Artikkel 24 Components of the ICT business continuity policy :

IKT-forretningskontinuitetspolitikken skal inneholde **bestemmelser** om

- styring og organisering for å implementere IKT-forretningskontinuitetspolitikken
- samsvar mellom IKT-forretningskontinuitetsplaner og generelle forretningskontinuitetsplaner
- utviklingen av IKT-forretningskontinuitetsplaner for alvorlige forretningsavbrudd som del av planene, og prioriteringen av IKT-forretningskontinuitetstiltak basert på en risikobasert tilnærming;
- utviklingen, testingen og gjennomgangen av IKT-respons- og gjenopprettingsplaner, i henhold bestemmelsene i artiklene 25 og 26;
- vurderingen av effektiviteten til implementerte IKT-forretningskontinuitetsarrangementer, planer, prosedyrer og mekanismer, i henhold til artikkel 26;
- gjennomgangen av effektiviteten til implementerte IKT-forretningskontinuitetsarrangementer, planer, prosedyrer og mekanismer, i henhold til Artikkel 26 i denne forskriften;
- tilpasning av IKT-forretningskontinuitetspolitikken til kravene til kommunikasjon DORA-lovgivningen

CHAPTER IV: ICT business continuity management (4)

Artikkel 24 Components of the ICT business continuity policy:

Det er særskilte krav for:

- Central counterparties / Sentrale motparter, jf. Artikkel 24 (2)
- Central securities depositories / Verdipapirsentraler, jf. Artikkel 24 (3)
- Trading venues / Handelsplasser , jf. Artikkel 24 (4)

CHAPTER IV: ICT business continuity management (5)

Artikkel 25 Testing of the ICT business continuity plans:

Denne artikkelen fokuserer på testing av IKT-forretningskontinuitetsplaner. Den beskriver kravene til testscenarier, inkludert simulering av potensielle forstyrrelser og switchover-scenarioer. Artikelen inneholder også krav til dokumentasjon og håndtering av eventuelle mangler som identifiseres under testing.

Testing skal

- baseres på testscenarier som simulerer potensielle forstyrrelser
- inneholde testing av IKT-tjenester levert av IKT-tredjeparts tjenesteleverandører
- inneholde scenarier for overføring fra primær IKT-infrastruktur til redundanskapasitet, sikkerhetskopier og redundante fasiliteter
- være utformet for å utfordre antakelsene som forretningskontinuitetsplanene
- inneholde prosedyrer for å verifisere evnen til den finansielle enhetens ansatte, IKT-tredjeparts tjenesteleverandører, IKT-systemer og IKT-tjenester til å svare tilstrekkelig på scenariene
- Testresultatene skal dokumenteres, og eventuelle identifiserte mangler skal analyseres, adresseres og rapporteres til ledelsesorganet.

Særskilte krav til

- Central counterparties / Sentrale motparter, jf. Artikkel 25 (3)
- Central securities depositories / Verdipapirsentraler, jf. Artikkel 24 (4)

CHAPTER IV: ICT business continuity management (6)

Artikkel 26 ICT response and recovery plans:
Denne artikkelen omhandler utviklingen av IT-respons- og gjenopprettingsplaner. Den beskriver kravene til disse planene, inkludert spesifikasjon av aktiverings- og deaktiveringsbetingelser, kortsiktige og langsiktige gjenopprettingsalternativer, og identifisering av relevante scenarier for alvorlige forretningsforstyrrelser.

Når finansielle enheter utvikler IKT-respons- og gjenopprettingsplanene skal de ta hensyn til resultatene av den finansielle enhetens driftskonsekvensanalyse (BIA).

(1) IKT-respons- og gjenopprettingsplanene skal
- spesifisere betingelsene som utløser aktivering eller deaktivering
- beskrive hvilke handlinger som skal tas for å sikre tilgjengelighet, integritet, kontinuitet og gjenoppretting, for minimum de IKT-systemer og -tjenester som støtter kritiske eller viktige funksjoner
- være utformet for å oppfylle gjenopprettingsmålene for driften
- være dokumentert og tilgjengelig for personalet og være lett tilgjengelig i tilfelle en nødsituasjon
- gi både kortsiktige og langsiktige gjenopprettingsalternativer, inkludert delvis systemgjenoppretting
- fastsette mål for IKT-respons- og gjenopprettingsplanene og betingelsene for å kunne konkludere om det var en vellykket utførelse av planene.

CHAPTER IV: ICT business continuity management (7)

Artikkel 26 ICT response and recovery plans:

(2) IKT-respons- og gjenopprettingsplanene skal identifisere relevante scenarier, inkludert scenarier med alvorlige forretningsforstyrrelser og økt sannsynlighet for forekomst av avvik. Foretaket skal ta hensyn til scenariene som framgår av Artikkel 26 (2), som blant annet er

- cyberangrep og overføringer mellom primær IKT-infrastruktur og redundanskapasitet, sikkerhetskopier og redundante fasiliteter
- delvis eller total svikt av lokaler, inkludert kontor- og forretningslokaler og datasentre
- vesentlig svikt av IKT-ressurser eller kommunikasjonsinfrastruktur
- ikke-tilgjengeligheten av et kritisk antall ansatte eller ansatte som har ansvar for å sikre kontinuiteten i driften
- omfattende strømbrudd

(3) For gjenopprettingstiltak som ikke er mulig på kort sikt grunnet kostnader, risiko, logistikk eller uforutsette omstendigheter, så skal IKT-respons- og gjenopprettingsplanene vurdere alternativer.

(4) Planen skal vurdere og implementere kontinuitetstiltak for å håndter redusere svikt hos IKT-tredjeparts tjenesteleverandører som leverer kritiske og viktige tjenester

CHAPTER V: Report on the ICT risk management framework review (1)

Article 27: Format and content of the report on the review of the ICT risk management framework

Artikkelen omhandler de detaljerte kravene som finansielle enheter må oppfylle når det gjelder utformingen og innholdet i rapporten som skal utarbeides etter vurdering av foretakets IKT-risikostyringsrammeverk.

(2) Rapporten har

(a) en introduksjons-del som beskriver

- foretaket og dets gruppestruktur,
- Litt om konteksten foretaket opererer i med tanke på tjenester, aktiviteter, organisasjon, kritiske funksjoner, strategi, store prosjekter, forholdet in-house og utkontrakterte tjenester og systemer m.m
- Oppsummering av de største endringene i IKT-risikostyringsrammeverket siden forrige rapport.
- et sammendrag av den nåværende og nærstående IKT-risiko profil, trussel landskap, vurdert effektivitet av kontrollene, og sikkerhetsstatusen til foretaket

CHAPTER V: Report on the ICT risk management framework review (2)

Article 27: Format and content of the report on the review of the ICT risk management framework

(b) til (e) – Ulike datoer, årsaken til vurderingen, hvilken funksjon som har gjort vurderingen, de størsdte endringene og forbedringer i IKT-Risikostyringsrammeverket

(f) en beskrivelse av de største endringene og forbedringene i IKT-risikostyringsrammeverket siden forrige gjennomgang;

(g) sammendrag av funnene fra gjennomgangen og detaljert analyse og vurdering av alvorligheten av svakheter, mangler og hull i IKT-risikostyringsrammeverket i løpet av gjennomgangsperioden;

(h) en beskrivelse av tiltakene for å adressere de identifiserte svakheter, mangler og hull med spesifikasjon av ytterligere detaljer

(i) Informasjon om videre utvikling av rammeverket

(j) Konklusjoner fra vurderingen av IKT Risk Management Framework

(k) informasjon om tidligere gjennomganger

(l) informasjon om kildene brukt i utarbeidelsen av rapporten

Kryptering (art. 6) og nøkkelhåndtering (art. 7)

POLICY som er basert på resultatet av en dataklassifisering

og som inneholder REGLER for

- kryptering av lagrede data og data under overføring
- kryptering av data i bruk. Eventuelt i egen, beskyttet omgivelse eller tilsvarende
- BESTEMMELSER om bruk, beskyttelse og livsløp når det gjelder nøkler
- kriterier for valg av løsning og praktisering av den
- kompenserende tiltak og overvåking skal begrunnes
- livsløp - generere, fornye, oppbevare, kopiere, arkivere, gjenfinne, overføre, deaktivere, og slette (artikkel 7)
- beskyttelse mot tap, uautorisert tilgang, utilsiktet eksponering og endring (artikkel 7)

Drift (art. 8)

Utvikle, dokumentere og implementere prosedyrer:

- beskrivelse: installering, vedlikehold, konfigurering, sletting. Parametre.
- kontroll og overvåking: sikkerhetskopiering/tilbakelegging, kjøresekvens, revisjonsspor og logging.
- skille utvikling og drift
- feilhåndering: protokoll, kontaktliste, omstart, tilbakelegging, gjennoppretting.

Kapasitet og ytelse (art. 9)

Utvikle, dokumentere og implementere prosedyrer:

- utnytte IT ressursene best mulig
- bedre tilgjengelighet til data og systemer
- planlegging, jf. lang leveringstid

Sårbarhet og oppdatering (art. 10)

Utvikle, dokumentere og implementere prosedyrer:

- inntrenging og uautorisert bruk
- automatisk skanning. Kritiske og viktige systemer skal skannes minst ukentlig.
- leverandører: I det minste rapportere kritiske sårbarheter og gi statistikk og trender. Plikt til å finne rotårsak og rette feil.
- kritiske og viktige systemer: spore bruken av 3. part bibliotek og open source. Versjon og oppdatering.
- opplyse om sårbarheter
- kriterier for å prioritere oppdateringer. Kontrollere at sårbarheter er lukket.
- sikkerhetsoppdateringer prosedyre: identifisere, vurdere, frister og hasterutiner

Datasikkerhet og systemsikkerhet (art. 11)

Utvikle, dokumentere og implementere prosedyrer:

- tilgangskontroll herunder programvare
- baseline konfigurasjon og kontroll opp mot denne. Bærbart. Skygge-IT
- sletting
- leverandører: resiliens, rollefordeling
- kompetanse og kapasitet

Logging (art. 12)

Utvikle, dokumentere og implementer prosedyre, protokoller og verktøy:

- hva, hvor lenge, oppbevaring, behandling, bruk
- tilstrekkelig detaljert til å avdekke uvanlig aktivitet
- administrasjon av brukere, logisk og fysisk tilgang
- kapasitet, endringsstyring, drift, nettverk
- beskytte loggene mot endring, sletting og uautorisert tilgang
- avdekke feil ved loggingen
- synkronisering av klokker

Nettverk (art. 13)

Utvikle, dokumentere og implementer policy, prosedyre, protokoller og verktøy:

- dokumentering av alle forbindelser og dataflyt
- segmentering. Admin nettverk.
- perimeterbeskyttelse.
- kryptering: bedriftsinterne nettverk, offentlige, nasjonale, tredjeparter, trådløse, internt
- brannmur: administrasjon og regler. Kontroll minst hver 6 måned for kritiske og viktige systemer.
- kontroll av arkitektur og sikkerhetsdesign årlig
- baseline sikerhetskonfigurasjon. Herding.
- levetid for sesjoner
- SLA på alle nivåer

Overføre Informasjon (art. 14)

Utvikle, dokumentere og implementer policy, prosedyre, protokoller og verktøy som sikrer at informasjonen er

- autentisk, tilgjengelig, uendret og beskyttet
- beskyttet mot uønsket innsyn (non-disclosure)
- beskyttet mot lekkasje

Mottatte spørsmål

Mottatte spørsmål

Med tanke på kravet til identifisering (og dokumentasjon) av kritiske og viktige funksjoner i selskapet. Hva er egentlig dokumentasjonskravet her? Hvor detaljert skal prosessene kartlegges? Er det for eksempel noen krav i DORA til nivå på prosessbeskrivelsene som lages?

Det er mange forpliktelser i DORA som åpenbart forutsetter en større aktør med et betydelig antall ansatte.

Eksempelvis:

- Plikt etter artikkel 13 for IKT-styring til å presentere rapporter til virksomhetens ledelse,
- Plikt etter artikkel 5 til å etablere interne rapporteringskanaler,
- Plikt etter artikkel 6 til å etablere en delvis uavhengig kontrollfunksjon
- Plikt etter artikkel 6 til å sikre skille og uavhengighet av IKT-risikostyringsfunksjoner, kontrollfunksjoner og interne revisjonsfunksjoner.

Ovennevnte og andre forpliktelser etter DORA synes ikke fornuftige for en virksomhet med færre enn 5 ansatte, hvor alle ansatte kommuniserer med hverandre daglig. Spørsmålet er om forholdsmessighetsprinsippet i artikkel 4 gir adgang til å bruke fornuft ved anvendelse av slike forpliktelser for virksomheter med veldig få ansatte, hvor denne formaliseringen av internt arbeid og kommunikasjon vil medføre ineffektivitet?

Lenke til norsk uoff. oversettelse av DORA

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

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY