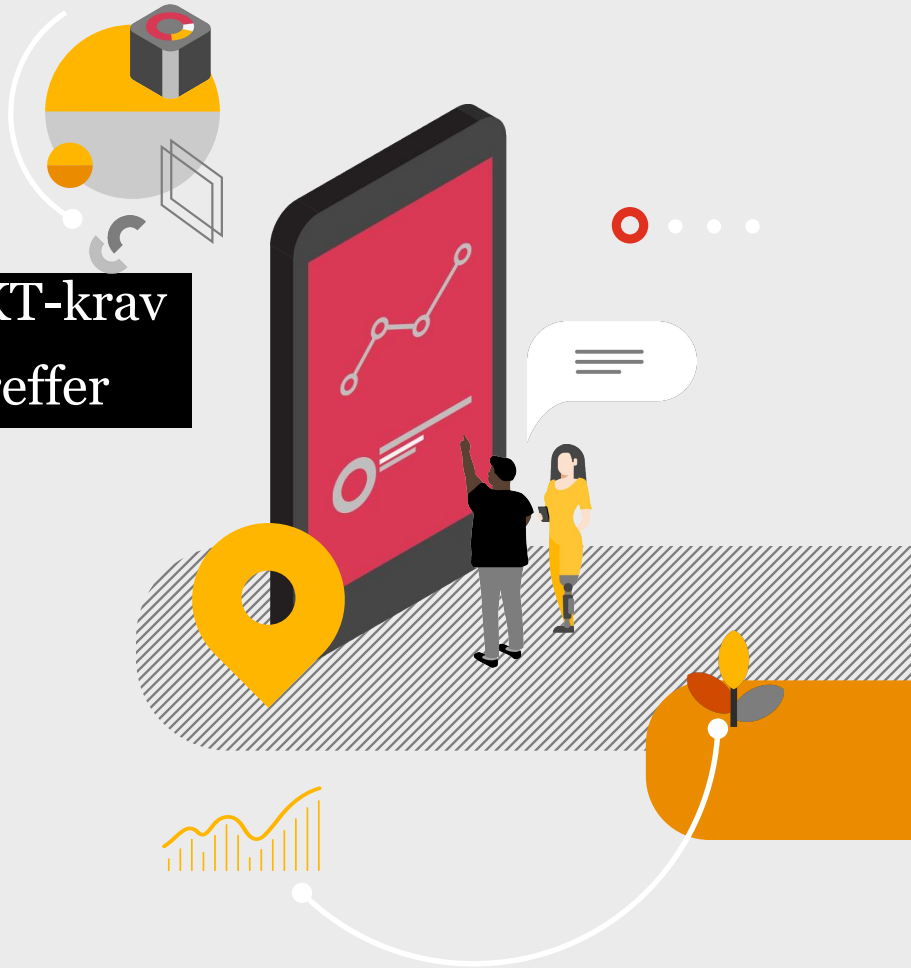
Etterleve morgendagens regulatoriske IKT-krav og compliance sin rolle når DORA intreffer

Digital Operational Resilience Act

Andreas Fredriksen - Manager, Risk Services i PwC

02. November 2023



1

DORA: Hva, hvorfor, når.

DORA i korte trekk

Finansnæringen står ovenfor hyppigere og mer komplekse cybertrusler. Det er flere og mer kompetente angripere, lengre verdikjeder og økende grad av digitale verdiforslag hos selskaper.

DORA er et detaljert og omfattende regelverk for digital operasjonell motstandskraft på EU-nivå.

Formålet er å **harmonisere** det regulatoriske landskapet knyttet til IT- og cyberrisiko i finansnæringen.

Ved å **standardisere regulatoriske krav** vil DORA sikre et felles nivå for digital operasjonell motstandskraft på tvers av virksomheter i den finansielle sektoren i EU og EØS området (inkl deres leverandører).

DORA


ESMA
European Securities and Markets Authority


eiopa
European Insurance and
Occupational Pensions Authority


EBA
EUROPEAN
BANKING
AUTHORITY

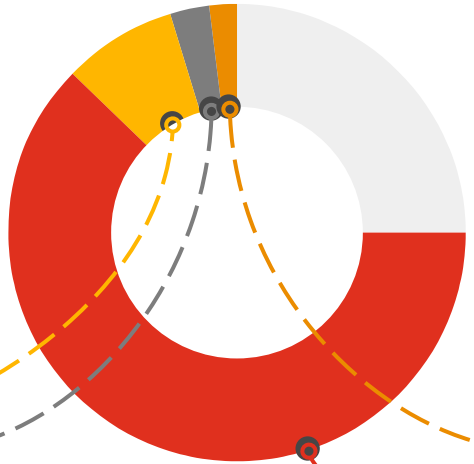
Hvem er trusselaktørene?

Spioner
For informasjonen

Eks. Statlige etterretningstjenester

Sabotører
For effekten

Eks. Insidere



Hacktivister
For saken

Eks. Anonymous

Kriminelle
For pengene

Eks. Conti

Hva gjør oss sårbare?

Manglende oversikt og beskyttelse av **kronjuveler og datagullet**, hva er viktig for deg og kan være interessant for angripere?

Utdatert IT med svakheter som angripere kan utnytte (eks manglende patching og oppdateringer).

Manglende **konfigurering** av infrastruktur for å motstå kjente angrep.

Manglende **"sikkerhetshygiene"** tillater angriper å ta kontroll. Eks brukerkontoer som ikke er tilstrekkelig sikret, to-faktor autentisering, monitorering, opplæring, osv.

Manglende innsikt i motstandsdyktighet modenhet og risikoappetitt gjør at man tar ubevisst risiko

Trussellandskap og case-studier fra finanssektoren

	Generiske trusler			Trusler i finanssektoren			
Cyber-trussel scenarioer	Ransomware kryptert data, trusler rettet mot lekkasje av sensitiv data	Økende kompleksitet og avhengighet av digital verdikjede	Økt fokus og målretting mot digital verdikjede	Svindel av midler fra institusjoner via e-post	Svindel av midler fra enkeltpersoner og institusjoner	Forstyrrelser av nettbaserte tjenester	ID-tyveri for å svindle enkeltpersoner
Nylige hendelser	**2021** **En falsk nettleseroppdatering førte til utpressing av 40 millioner dollar fra CNA Financials**	**2021** **Sårbarhet i eldre Accellion FTA-programvare ble brukt i datautpressing av TA505**	**2022** **Over 570 tusen dollar ble stjålet etter et kompromiss med DNS -infrastrukturen**	**2020** **Angripere arrangerer uredelig overføring av $10 millioner fra Norfund gjennom kompromitterte e-poster**	**2022** **Nord-Korea-baserte trusselaktører stjal 100 millioner dollar ved å utnytte en sårbarhet i Horizon Bridge-blokkjeden**	**2022** **Den pro-russiske hacktivisten Killnet lanserte DDoS-angrep mot JP Morgan.** **- flere norske foretak truffet av samme**	**2022** **Datainnbrudd førte til at personopplysninger til 50 000 kunder ble kompromittert**

DORAs fem pilarer

IKT-risikostyring

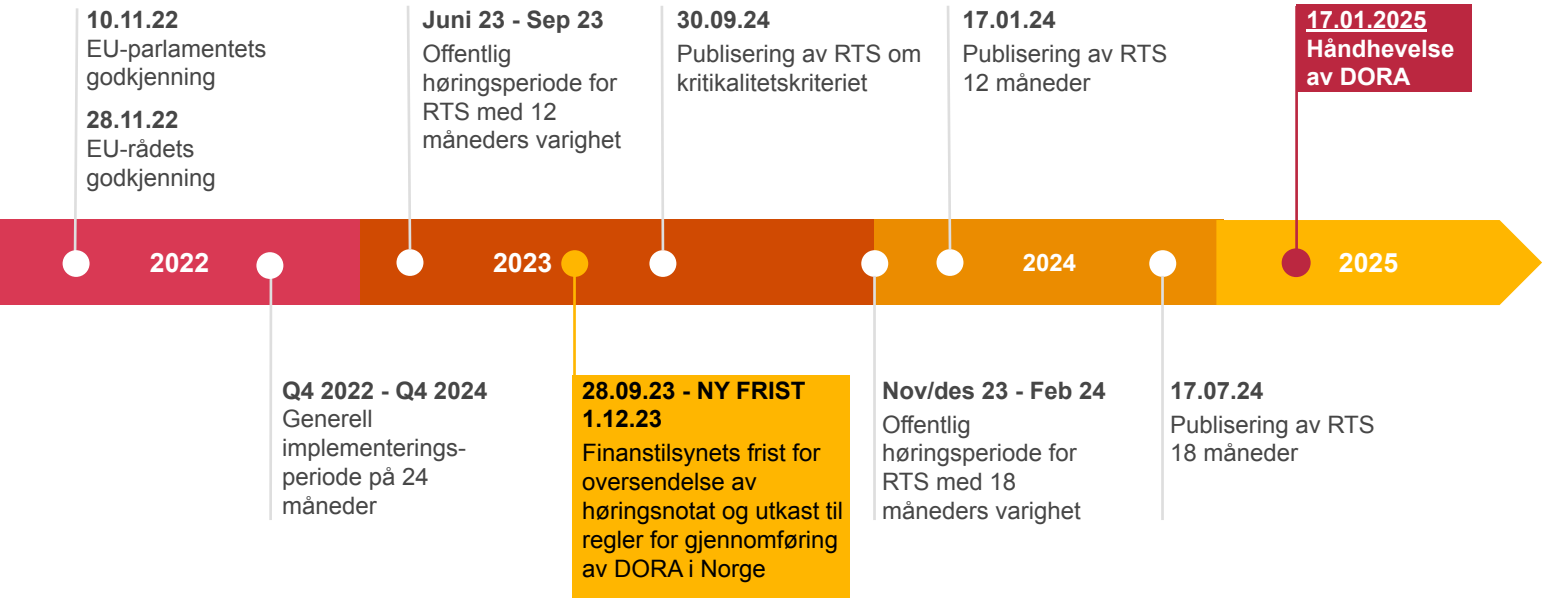
Hendelses-rapportering

Testing

Risikostyring av tredjeparter

Informasjonsdeling

Den regulatoriske tidslinjen



RTS 12 måneder

- RTS - IKT RMF
- RTS - IKT om forenklet IKT RMF
- RTS - IKT Policier
- RTS om klassifisering av store IKT hendelser
- ITS om informasjonsregisteret

RTS 18 måneder

- RTS om underleverandører
- RTS om rapportering av store IKT-hendelser

2

DORA vs. gjeldende regelverk

Fra IKT-forskriften til DORA

Kilde: Risiko- og sårbarhetsanalyse (ROS) 2023

I Norge reguleres bruken av IKT innen finanssektoren i hovedsak gjennom IKT-forskriften. For noen foretakstyper reguleres bruken av IKT i særregelverk. Videre reguleres Finanstilsynets tilsynsaktiviteter gjennom finanstilsynsloven.

DORA gjelder alle finansielle organisasjoner og har betydelig overlapp med IKT-forskriften og finanstilsynsloven. Likevel går DORA bestemmelser enda dypere ved å pålegge strengere krav til dokumentasjon, mer detaljerte standarder og ikke minst en strengere struktur for sanksjoner.

DORA omfatter flere aktører enn IKT-forskriften og får anvendelse innenfor hele EØS-området…

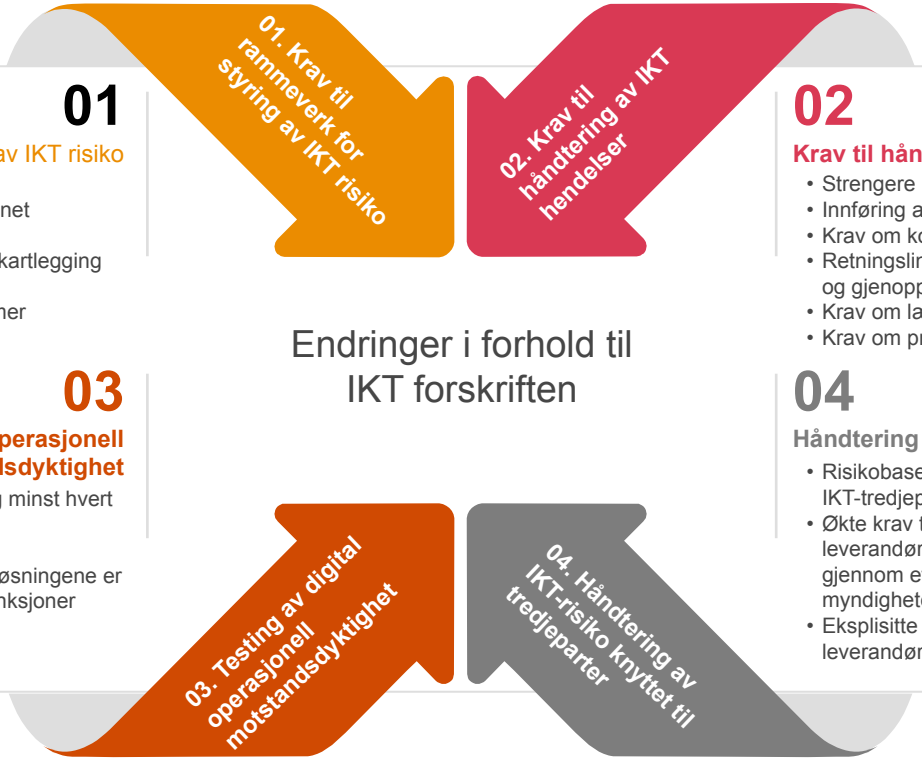
IKT-forskriften

- Banker
- Kredittforetak
- Finansieringsforetak
- Forsikringsforetak
- Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond
- Børser og autoriserte markedsplasser
- Inkassoforetak
- Eiendomsmeglerforetak
- Betalingsforetak og opplysningsfullmektiger
- E-pengeforetak
- Systemer for betalingstjenester

DORA

- Kredittinstitusjoner
- Betalingsinstitusjoner
- Leverandører av kontoinformasjonstjenester
- Elektroniske pengeinstitusjoner
- Kapitalforvaltningsforetak
- Tjenesteleverandører av kryptoaktiva, utstedere av kryptoaktiva, utstedere av aktiva-refererte tokens og utstedere av betydelige aktiva-refererte tokens
- Verdipapirsentraler
- Sentrale motparter
- Handelsplasser
- Transaksjonsregister
- AIF-forvaltere
- Forvaltningsselskaper
- Tjenesteleverandører for datarapportering
- Forsikrings- og gjenforsikringsforetak
- Forsikringsformidlere, gjenforsikringsformidlere og tilhørende forsikringsformidlere
- Institusjoner for tjenestepensjon
- Kredittvurderingsbyråer
- Administratorer av kritiske benchmarks
- Crowdfunding tjenesteleverandører
- Verdipapiriseringsdepoter
- IKT tredjeparts tjenesteleverandører

DORA i forhold til IKT-forskriften



01

Krav til rammeverk for styring av IKT risiko

- Etablere rammeverk for risikostyring
- Regelmessig opplæring av styringsorganet
- Regelmessig revisjon fra IKT-revisorer
- Identifikasjon av IKT-systemkontoer og kartlegging av fysisk utstyr
- Årlig risikovurdering av eldre IKT-systemer

02

Krav til håndtering av IKT hendelser

- Strengere krav til oppdagelsesmekanismer.
- Innføring av IKT Business Continuity Policy
- Krav om konsekvensanalyse
- Retningslinjer for sikkerhetskopiering, gjenoppretting og gjenopprettingsmetoder
- Krav om læring og utvikling
- Krav om prosesser for IKT-relaterte hendelser

03

Testing av digital operasjonell motstandsdyktighet

- Krav om Threat-Led Penetration Testing minst hvert 3 år
- Involvering av trejdepartsleverandører
- Krav om jevnlig testing av hvor robust løsningene er og som sikrer at kritiske systemer og funksjoner testes årlig

04

Håndtering av IKT-risiko knyttet til tredjeparter

- Risikobasert tilnærming ved inngåelse av avtaler med IKT-tredjepartstjeneste leverandører
- Økte krav til styring og kontroll med tredjeparter. Visse leverandører vil klassifiseres som 'kritiske' og følges opp gjennom et eget opplegg som styres av sentrale EU myndigheter (lead overseer EBA, EIOPA eller ESMA)
- Eksplisitte krav til avtalene med IKT-tredjeparts-leverandører

Refleksjoner fra etablerte aktører

Hva tenker aktørene i finansnæringen?

Dårlig med tid og ressurser…

Sliter med med å tolke regelverket..

DORA gjenspeiles i IKT-forskriften, MEN er langt mer krevende

Blir det sanksjoner?

Svært krevende for de mindre bankene

Samarbeidet mellom finansnæringen og tilsynsmyndighetene er i endring

DORA blir en større omveltning enn GDPR

Etterlyser samarbeid om hvordan man skal håndtere leverandører i næringen. Kritiske leverandører?

Ønsker konkret veiledning og standardmaler (operasjonalisering)

3

Observasjoner

Modenhetsvurderinger - Observasjoner fra kunder

- Behov for ytterligere formalisering og mer detaljert dokumentering
- Ytterligere dokumentering av beredskapsplan
- Ytterligere formalisering og forankring av prosesser til ledelsen
- Heve kompetansenivået og sikre etterlevelse av policyer
- Manglende fokus på risiko ifm. legacy IT.
- Manglende gjennomføring av BIA

- Behov for formalisering av prosessen for håndtering og rapportering
- Behov for ansvarliggjøring av håndtering og rapportering av ulike typer for hendelser

- Manglende skriftlig dokumentasjon og policyer for å formalisere allerede implementerte tiltak og rutiner

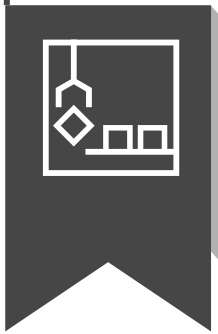
- Behov for bedre struktur og systemstøtte vedr. Gjennomføring og oppfølging av pentester
- Manglende rolle- og ansvarsfordeling for å sikre effektiv oppfølging av testregimet

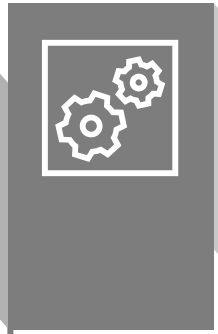
- Styrke due diligence av tredjeparter
- Manglende exit-krav i leverandørkontrakter
- Manglende oppfølging av tredjepartsrisiko
- Manglende eller feil risikoverdi av tredjeparter
- Manglende strukturert oppfølging av tredjeparter innen informasjonssikkerhet
- Leverandørstyringen må styrkes dersom virksomheten ønsker å forbedre styringen av informasjonssikkerhet
- Mangel på riktige kontroller for å sikre at leverandøren har og sørger for nødvendige sikkerhetsnivå for virksomheten

Finanstilsynets observasjoner og vurderinger

Kilde: Risiko- og sårbarhetsanalyse (ROS) 2023

Utkontraktering
-Mangelfull oppfølging av leverandører
-Manglende involvering i leverandørens test av kriseløsninger



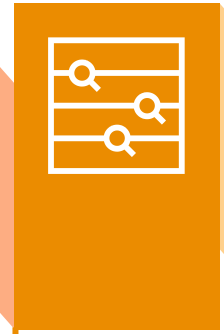


Manglende IKT kompetanse
I 2022 påpekte tilsynet behovet for tilstrekkelig IKT-kompetanse og uavhengige kontrollfunksjoner i andrelinjen, som bør utføre selvstendige vurderinger og kontroller av IKT-området.

Manglende forretningsmessige konsekvensanalyser
Mange foretak mangler/har mangelfulle BIA, som er avgjørende for beredskaps- og kriseplanlegging, inkludert utkontrakterte tjenester.

Datakvalitet
Behov for et datastyringsrammeverk, spesielt for større foretak, for å sikre datakvalitet og hindre misbruk. Det ble også observert manglende klassifisering av informasjon og risikovurdering ved datatap.

Tilsyn med overvåkningssystemer
Mangler i bankenes overvåking av transaksjoner knyttet til AML og terrorfinansiering, inkludert manglende sjekk av kundedata og bransjeregler, samt behov for bedre tilpasning mellom AML-regler og risikoanalyser.



Tilsyn med betalingsforetak
Manglende rutiner for sikkerhetsrelaterte kundeklager og behovet for kontaktinformasjon til brukerne, samt begrensninger i brukernes mulighet til å kommunisere effektivt med foretaket.

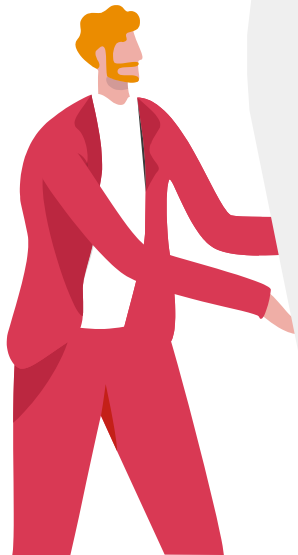
Leverandøroppfølging av tilgangsstyring

Kilde: Risiko- og sårbarhetsanalyse (ROS) 2023

I 2022 fulgte Finanstilsynet opp en sikkerhetshendelse fra 2021 der leverandørens ansatte misbrukte tilganger til ikke-tjenstlige data. Dette ble gjort for alle foretak som benyttet leverandøren. Finanstilsynet har også vurdert foretakenes rutiner for å følge opp IKT-tjenesteleverandører, spesielt knyttet til tilgangsstyring. Resultatene indikerer behov for bedre rutiner for å avdekke tilgangsmisbruk, samt mangler i foretakenes styring og kontroll av tilgangsrettigheter ved utkontrakterte tjenester. Det forventes at foretakene tar nødvendige tiltak for å forbedre tilgangsstyring og kontroll.

Etterlevelse av IKT-forskriften

Kilde: Risiko- og sårbarhetsanalyse (ROS) 2023



Finanstilsynet avdekket flere mangler knyttet til utkontraktering av IKT-virksomhet under tilsyn i 2022. Manglene inkluderte brudd på meldepliktforskriften ved foretakenes unnlatelse av å vedlikeholde en fullstendig oversikt over kontrakter knyttet til utkontraktering. Videre ble det registrert mangler i overholdelsen av IKT-forskriften § 2, fjerde ledd, som foreskriver at avtaler knyttet til utkontraktering av IKT-virksomhet, samt eventuelle endringer i slike avtaler, skal være gjenstand for styrebehandling i foretakene.

Tilsynsrapportene indikerte også tilstedeværelsen av kontrakter for utkontraktering som ikke oppfylte de fastsatte kravene i IKT-forskriften § 12. Denne forskriften spesifiserer at slike avtaler bør sikre at foretak underlagt tilsyn har rett til å inspisere og revidere aktiviteter som utføres av leverandøren i forbindelse med avtalen. Videre skal slike avtaler gi Finanstilsynet tilgang til nødvendig informasjon og tilsyn hos IKT-leverandøren, når det anses som nødvendig som en del av tilsynsprosessen med foretaket.

4

Hva bør virksomheten din fokusere på?

Styrets ansvar

Som en del av den helhetlige risikostyringen bør styret diskutere risiko relatert til informasjonssikkerhet. Styret bør:

- ➔ Fastsette virksomhetens risikotoleranse
- ➔ Forsikre seg om at det er lagt en god strategi for å overvåke, identifisere og håndtere IKT-risiko og -hendelser.

Informasjonssikkerhet må være på agendaen til styret, og må være en prioritet for styreleder. Vi ser likevel at styret har utfordringer med å forstå risiko samt hvordan de skal ansvarliggjøre ledelsen. Styret må se på informasjonssikkerhet som en kritisk faktor for å:

- ➔ Lykkes med strategiske prioriteringer
- ➔ Opprettholde godt omdømme
- ➔ Ivareta drift av kritiske forretningsprosesser

Styret bør stille ledelsen spørsmål om styring, organisering, risiko og fremtidige investeringer.

Les mer i Styreboken 2023 fra PwC Norge, eller på https://www.pwc.no/no/pwc-aktuelt/dora-alt-du-trenger-a-vite.html

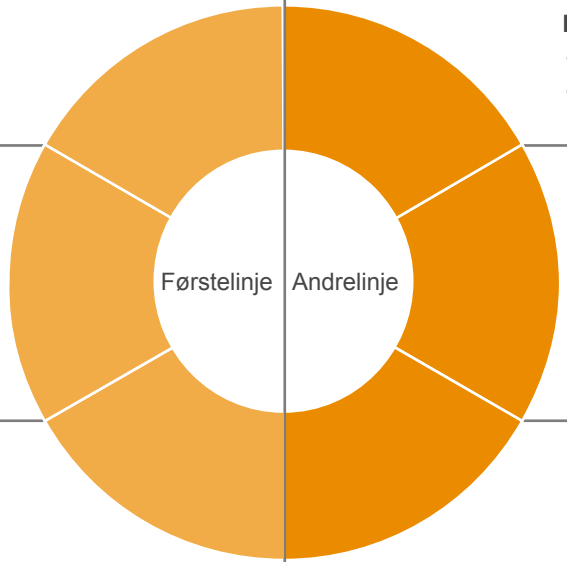
DORA krever økt kompetanse og oppfølging i linjene

Det stilles strengere krav til kompetanse, internkontroll og rapportering for finansforetak. Dette medfører strengere krav til styret og ledelse, samt betydelige forbedringer innen internkontroll, prosedyrer, hendelses-og myndighetshåndtering

Elementer i Virksomhetsplanlegging
- Definere virksomhetens kritiske funksjoner
- Strategier for forretningskontinuitet
- Policier, rutiner og prosedyrer

Varslingsrutiner og Implementering av Teknologi
- Utarbeide varslingsrutiner for internt og eksternt bruk
- Implementere teknologiske løsninger

Operativ Motstandstesting og Gjenoppretting
- Operativ motstandstesting
- Verktøy og metoder for datagjenoppretting



Effektiv Risikohåndtering: Risikoapetitt og Overvåkning
- Definere risikoapetitt og motstandsstrategi
- Overvåke og monitorere risikoer

Styringsrappotering og Policyprosesser
- Rapportering til ledelsen og styret

Kritisk Funksjonskartlegging og Risikovurdering
- Kartlegge kritiske funksjoner og tredjeparter
- Gjennomføre risikovurderinger

Compliancefunksjonens ansvar og oppgaver

- Foreslå rammeverk for etterlevelsesrisikoer
- Risikobasert arbeidsplan for overvåking og testing av etterlevelse
- Identifisere, vurdere og overvåke vesentlige etterlevelsesrisikoer
- Uavhengig rapportering
- Risikovurdering av nye produkter, tjenester og andre aktiviteter
- Gi råd og anbefale tiltak for å sikre etterlevelse
- Opplæring av ledelsen og ansatte vedr. etterlevelsesrisiko

Etterlevelse av DORA vil kunne utgjøre en etterlevelsesrisiko

Compliancefunksjonens ansvar og oppgaver

- Foreslå rammeverk for etterlevelsesrisikoer
- Risikobasert arbeidsplan for overvåking og testing av etterlevelse
- Identifisere, vurdere og overvåke vesentlige etterlevelsesrisikoer
- Uavhengig rapportering
- Risikovurdering av nye produkter, tjenester og andre aktiviteter
- Gi råd og anbefale tiltak for å sikre etterlevelse
- Opplæring av ledelsen og ansatte vedr. etterlevelsesrisiko

Testing av virksomhetens IKT-systemer og -sikkerhet

Compliancefunksjonens ansvar og oppgaver

Foreslå rammeverk for etterlevelsesrisikoer

Risikobasert arbeidsplan for overvåking og testing av etterlevelse

Identifisere, vurdere og overvåke vesentlige etterlevelsesrisikoer

Uavhengig rapportering

Risikovurdering av nye produkter, tjenester og andre aktiviteter

Gi råd og anbefale tiltak for å sikre etterlevelse

Opplæring av ledelsen og ansatte vedr. etterlevelsesrisiko

- Rapportere på etterlevelsesforhold knyttet til DORA

- IKT-hendelser

Risikostyringsfunksjonens ansvar og oppgaver

- Foreslå og følge opp foretakets overordnede risikostyringsrammeverk
- Aktivt involvert i utarbeidelsen av foretakets risikostrategi
- Aktivt involvert i foretakets prosess for risikovurderinger
- Sikre at alle vesentlige risikoer måles, styres og rapporteres
- Måle, overvåke, rapportere og rådgi
- Overvåke risikoeksponeringer, eskalere brudd
- Regelmessig rapportering til ledelsen om risikobildet og mulige risikoer

Mer konkrete krav til virksomhetens risikostyringsrammeverk på IKT-området

Risikostyringsfunksjonens ansvar og oppgaver

Foreslå og følge opp foretakets overordnede risikostyringsrammeverk

Aktivt involvert i utarbeidelsen av foretakets risikostrategi

Aktivt involvert i foretakets prosess for risikovurderinger

Sikre at alle vesentlige risikoer måles, styres og rapporteres

Måle, overvåke, rapportere og rådgi

Overvåke risikoeksponeringer, eskalere brudd

Regelmessig rapportering til ledelsen om risikobildet og mulige risikoer

- Risikostyring skal bidra i IKT-relaterte risikovurderinger for å identifisere, styre og rapportere risikoer i henhold til risikostyringsrammeverket.

- Krav om tilstrekkelig kompetanse på alle riskoområder, herunder IKT-området i andrelinjefunksjonene

Risikostyringsfunksjonens ansvar og oppgaver

Foreslå og følge opp foretakets overordnede risikostyringsrammeverk

Aktivt involvert i utarbeidelsen av foretakets risikostrategi

Aktivt involvert i foretakets prosess for risikovurderinger

Sikre at alle vesentlige risikoer måles, styres og rapporteres

Måle, overvåke, rapportere og rådgi

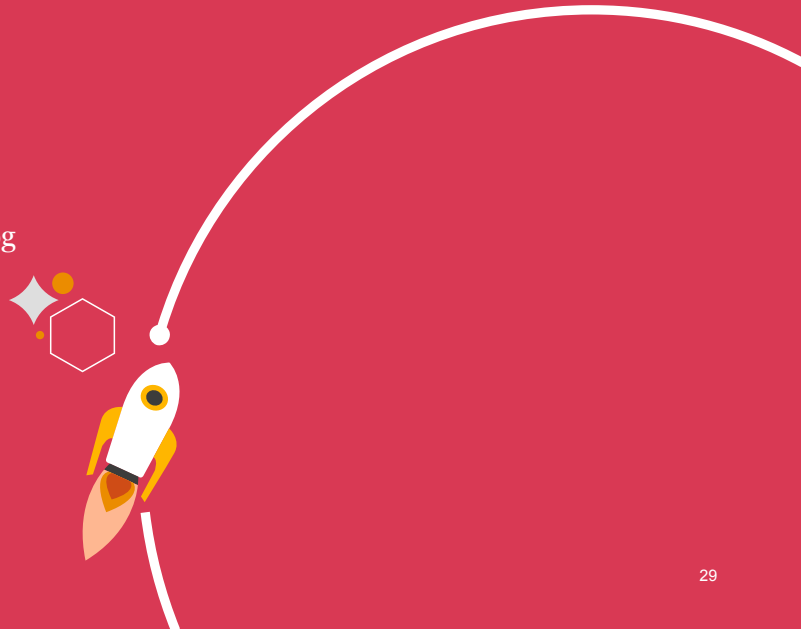
Overvåke risikoeksponeringer, eskalere brudd

Regelmessig rapportering til ledelsen om risikobildet og mulige risikoer

Gjelder også IKT-området, feks Cyber-risikoer og trender

De første fire tingene dere bør gjøre

1. Initiere vurdering av hva betyr DORA for dere? (gap-analyse) Hvis det er gjort allerede - koble deg på!
2. Vurdere kompetanse og kapasitet i de tre forsvarslinjene, evt behov for upskilling?
3. Sørge for at IT-risiko blir integrert i risikorammeverket samt at IKT-forskriften og DORA er på kartet for compliancerisikovurderinger
4. Opplæring/rådgivning: Vurdere fremtidige (risk -) og complianceaktiviteter på området, som først og fremst er opplærings- og implementeringsaktiviteter og være en rådgiver internt



Takk for meg!

Kontakt meg gjerne på
andreas.fredriksen@pwc.com
+47 952 61 075

pwc.no