STYRING AV IKT-TREDJEPARTSRISIKO I FINANSNÆRINGEN

Veileder

2025

Finans Norge

Forord

I en stadig mer digitalisert verden er finansnæringens evne til å håndtere IKT-tredjepartsrisiko avgjørende for å opprettholde stabilitet og tillit i markedet. Digital Operational Resilience Act (DORA) markerer et viktig steg for å sikre at finansinstitusjoner kan motstå, reagere på og gjenopprette normal drift etter IKT-relaterte forstyrrelser.

DORA stiller krav til en strukturert og helhetlig tilnærming til IKT-tredjepartsrisiko. Dette er ikke bare et regulatorisk krav, men også del av vårt samfunnsoppdrag. Vi må raskt kunne tilpasse oss teknologiske endringer og nye regulatoriske forventninger, samtidig som vi sikrer at våre tjenester forblir robuste og pålitelige.

Tilgang til relevant data og innsikt i tredjepartsleverandørers IKT-systemer er avgjørende for å lykkes med dette. Mange aktører i norsk finansnæring har allerede iverksatt omfattende tiltak for å styrke sin digitale motstandskraft.

For at tiltakene skal være effektive, må de være sammenlignbare og gjenkjennbare på tvers av aktører i næringen og i hele leverandørkjeden. Denne veilederen har som mål å være et praktisk verktøy for finansforetak som ønsker å styrke sin styring av IKT-tredjepartsrisiko. Den skal også bidra til standardisering av praksis og styrke samarbeid i bransjen.

Første versjon av denne veilederen ble lansert 17. februar 2025, og Finans Norge har en ambisjon om å videreutvikle den i takt med medlemmenes behov og internasjonale utviklingstrender.

Mer enn 20 personer med spisskompetanse fra Finans Norges medlemsorganisasjoner innen bank og forsikring har bidratt til utarbeidelsen av denne veilederen. I tillegg har PwC støttet oss i arbeidet. Jeg vil rette en stor takk til alle som har delt sin tid, innsikt og engasjement underveis i prosessen.

Pål Christian Waag

Finans Norge, fagdirektør cybersikkerhet

Innhold

1. Formål med veilederen

Formålet med veilederen er å hjelpe virksomheter i finansnæringen med å styre tredjepartsrisiko på en systematisk og effektiv måte, i tråd med kravene i DORA (Digital Operational Resilience Act). IKT-leverandører spiller ofte en kritisk rolle i finanssektoren, og mangelfull styring kan medføre betydelige risikoer knyttet til sikkerhet, kvalitet og etterlevelse.

Finansnæringen er definert som en samfunnskritisk funksjon, noe som innebærer et særlig ansvar for å beskytte operasjonell stabilitet og sikre kontinuitet i tjenestene. Ettersom mange virksomheter i sektoren er avhengige av leverandører og underleverandører for kjernefunksjoner som IT-infrastruktur, databehandling og kundetjenester, er det avgjørende med en strukturert tilnærming til risikostyring.

Moderne leverandørkjeder er preget av flere nivåer med avhengigheter. Effektiv styring av tredjepartsrisiko krever en tilnærming som går utover isolert vurdering av enkeltleverandører og inkluderer en grundig analyse av hvordan ulike aktører påvirker hverandre i verdikjeden. For å oppnå en helhetlig forståelse av den samlede risikoprofilen, bør virksomheter også identifisere og vurdere risiko knyttet til underleverandører. En slik tilnærming legger grunnlaget for mer presise risikovurderinger og styrker virksomhetens evne til å ivareta operasjonell robusthet gjennom proaktiv leverandøroppfølging.

Denne veilederen skal støtte virksomhetene i deres arbeid med:

- **Systematisk styring**: Virksomhetene får hjelp til å identifisere og vurdere risikoer knyttet til IKT-leverandører, samt å etablere effektive kontrolltiltak for å sikre at leverandører og underleverandører oppfyller nødvendige krav.
- **Etterlevelse av regelverk:** Veilederen hjelper virksomhetene med å oppfylle regulatoriske krav i DORA, med særlig fokus på krav som gjelder for styring og overvåking av IKT-leverandører.
- **Beskyttelse av kritiske prosesser:** Redusere sannsynligheten for at feil eller sikkerhetsbrudd hos IKT-leverandører og underleverandører får alvorlige konsekvenser for virksomhetens drift. Eksempelvis gjennom etablering av definerte krav i avtaler som omhandler kontinuerlig overvåking av leverandørers sikkerhetspraksis.

Ved å bruke denne veilederen kan finansvirksomheter balansere kravene til sikkerhet og effektivitet, samtidig som de opprettholder høye standarder for kvalitet og driftskontinuitet. Den gir også en felles referanseramme som kan styrke samarbeidet på tvers av bransjen og bidra til bedre oppfølging av leverandørforhold.

2. Hvordan er veilederen bygget opp?

Denne veilederen gir en overordnet innføring i styring av tredjepartsrisiko med et særlig fokus på sikkerhet, risiko og DORA. Veilederen er utformet for å hjelpe aktører i finansnæringen med å identifisere, vurdere, overvåke og håndtere risiko knyttet til tredjepartsforhold. Den tar utgangspunkt i livssyklusen til en tredjepartsrelasjon og dekker de fem hovedfasene:

1. **Planlegging:** Forberedelse og identifisering av behov og risiko knyttet til oppgaveleveransen.
2. **Vurdering og valg av leverandør:** Vurdering og valg av IKT-leverandører basert på risiko og krav.
3. **Avtaleinngåelse og oppstartsfase:** Etablering av tydelige krav i kontrakter og hva man bør tenke på for å sikre effektive prosesser ved etablering av tjenester med IKT-leverandører.
4. **Kontinuerlig oppfølging og overvåkning:** Beskrivelse av tilnærming og hjelpemiddel for løpende overvåking og evaluering av tredjepartsytelse og risiko.
5. **Exit-strategi og avslutning av samarbeidet:** Planlegging og gjennomføring av en strukturert avslutning av leverandørforhold når nødvendig.

Veilederen inkluderer praktiske sjekklister, maler og standarder som kan anvendes for å styrke risikostyringsprosessene. Hvert kapittel gir detaljerte beskrivelser av hvilke tiltak som bør gjennomføres og hvordan disse kan tilpasses ulike typer leverandørforhold, med fokus på etterlevelse av DORA-kravene. Tiltakene belyses fra flere perspektiver, inkludert juridiske krav, identifiserte risikoer og beste praksis for å sikre en helhetlig styring av leverandørrelasjoner. Medlemsbedriftene må selv vurdere hvilke steg og tiltak som er relevante og nødvendig i den enkelte prosess, og som er anvendelige for den enkelte bedrift.

Ved behov for konkret rådgivning, ta kontakt med Pål Christian Waag, fagdirektør cybersikkerhet i Finans Norge.

For mer informasjon, se: DORA, kapittel 5, artikkel 28-30 og RTS Third-Party ICT Service Policy, artikkel 5

3. Hva er tredjepartsrisikostyring?

Tredjepartsrisikostyring er prosessen med å identifisere, vurdere, overvåke og redusere risiko forbundet med bruk av eksterne leverandører. Målet med denne prosessen er å minimere risikoen for negative konsekvenser ved avvik, forbedre operasjonell effektivitet og tilrettelegge for samarbeid og innovasjon.

Tidligere fokuserte IKT-forskriften på begrepet "utkontraktering" for å regulere hvordan virksomheter håndterer overføring av IKT-funksjoner til eksterne leverandører. Dette omfattet spesifikke krav til vurdering, oppfølging og rapportering knyttet til utkontrakterte tjenester.

Med innføringen av DORA har reguleringene blitt utvidet fra å fokusere utelukkende på "utkontraktering" til å omfatte et bredere spekter av risiko relatert til eksterne IKT-leverandører. Gjennom begrepet "ICT Third-Party Service Providers" legges det særlig vekt på "ICT Third-Party Risk". Denne tilnærmingen inkluderer både tradisjonell utkontraktering, bruk av konserninterne IKT-leverandører og andre former for IKT-tjenestekjøp fra tredjeparter, og reflekterer en helhetlig forståelse av risiko knyttet til alle eksterne IKT-leverandører.

Konserninterne IKT-leverandører (Intra-Group ICT Service Providers) er selskaper innenfor samme konsern eller allianse som leverer IKT-tjenester til andre enheter i konsernet. Disse er underlagt konsernstyring og er dermed enklere å følge opp.

Konserninterne IKT-leverandører er underlagt de samme rapporterings- og sikkerhetskravene som eksterne IKT-leverandører, spesielt når de støtter kritiske eller viktige funksjoner. Dette innebærer blant annet at kontraktuelle avtaler må være tydelig dokumentert, og at datahåndtering skjer i samsvar med kravene i DORA. Videre må konserninterne IKT-leverandører inkluderes i IKT-tjenesteverdikjeden og rapporteres i henhold til DORA-kravene. Blant annet krever DORA at alle relevante underleverandører som støtter kritiske funksjoner, identifiseres og overvåkes.

Det er viktig å merke seg at styringsmulighetene over konserninterne IKT-leverandører ofte er bedre enn over eksterne IKT-leverandører. Siden de opererer innenfor samme konsern, er det mulig å ha

større grad av kontroll og innsyn i virksomheten, noe som kan bidra til å redusere risiko og forenkle oppfølgingen, men på den annen side er sannsynligvis exit-planer mer krevende å iverksette.

Styring av tredjepartsrisiko innebærer å sikre at eksterne partnere og IKT-leverandører leverer tjenester i samsvar med avtalte betingelser, kvalitetskrav, sikkerhetsstandarder og regulatoriske krav. Dette omfatter hele prosessen fra valg av IKT-leverandører til oppfølging av deres ytelse og etterlevelse gjennom hele kontraktsperioden. Samtidig kan bruken av eksterne leverandører øke kompleksiteten og skape et mer sammensatt risikobilde. Dette krever grundigere styring, inkludert vurdering av leverandørens sikkerhetstiltak og risikohåndtering for å redusere risikoen for driftsforstyrrelser og sikkerhetsbrudd.

Et sentralt element i DORA er skillet mellom "vanlige" IKT-tjenester og "kritiske eller viktige" tjenester. Kritiske og viktige tjenester er underlagt strengere krav, da de har potensial til å påvirke virksomhetens operasjonelle motstandskraft betydelig. Eksisterende retningslinjer fra de europeiske tilsynsmyndighetene (ESA), som ESMA Cloud Guidelines og EBA Guidelines for utkontraktering, forventes fortsatt å være relevante, mens DORA styrker disse ved å spesifisere krav til risikohåndtering for kritiske leveranser.

Hva innebærer tredjepartsrisikostyring?

- **Identifikasjon av risiko:** Forstå hvilke risikoer som kan oppstå ved å involvere eksterne parter, for eksempel datainnbrudd, operasjonelle utfordringer eller juridiske problemer
- **Risikovurdering:** Analysere sannsynligheten og konsekvensene av de identifiserte risikoene. Dette kan inkludere å evaluere IKT-leverandørens sikkerhetspraksis, økonomiske situasjon, og deres evne til å levere tjenester i henhold til avtaler.
- **Risikoreduserende tiltak:** Implementere sikkerhetstiltak og kontrollmekanismer som sikrer at IKT-leverandøren oppfyller virksomhetens standarder og krav
- **Kontinuerlig overvåking:** Opprettholde en løpende dialog og evaluering av IKT-leverandørens ytelse og samsvar med avtalte vilkår. Dette inkluderer regelmessig innhenting av rapporter, leverandørrevisjoner og en åpen dialog for å adressere eventuelle utfordringer som oppstår.
- **Exit/mulighet til å bytte IKT-leverandør:** Utforme tydelige prosedyrer og kontraktsfestede mekanismer for å sikre en smidig avslutning av samarbeidet med en leverandør dersom krav og forventninger ikke innfris. Dette innebærer å ha en detaljert plan for overføring av data og tjenester, samt tiltak for å minimere driftsavbrudd og sikre kontinuitet ved overgang til en ny leverandør.

For mer informasjon, se: DORA, kapittel 1, artikkel 3, kapittel 2, kapittel 5, artikkel 28, artikkel 31, ITS on Register of Information og RTS on Risk Management Framework.

4. Hvordan jobbe helhetlig med styring av IKT-tredjepartsrisiko

En sentral del av arbeidet innebærer å etablere en oversikt over alle IKT-leverandører og underleverandører, som oppdateres løpende ved endringer. I tillegg må virksomheten gjennomføre systematiske konsekvensanalyser for virksomheten (Business Impact Analysis, BIA) for å identifisere kritiske IKT-leverandører og funksjoner, eksempelvis ved bruk av standarder som ISO 22317 eller lignende. Dette bidrar til å avdekke konsekvenser ved uønskede hendelser og danner grunnlaget for å etablere kontinuitets- og kriseplaner. For å sikre en konsekvent vurdering bør analysene være i tråd med spesifikke krav i DORA, som omhandler gjennomføring av konsekvensanalyser for virksomheten, samt risikovurdering av IKT-leverandører og underleverandører.

Videre er det viktig å utvikle tydelige krav og retningslinjer for valg og evaluering av leverandører. Disse skal sikre at leverandører møter forventningene til kvalitet, sikkerhet og kontinuitet.

I avtaleperioden er det avgjørende å etablere mekanismer for løpende oppfølging og kontroll. Dette inkluderer kontinuerlig overvåking av tredjepartsrisiko, systematisk dokumentasjon av funn og tiltak, jevnlig revisjon av tredjepart samt egne prosesser og rutiner for å sikre samsvar med regulatoriske krav.

En helhetlig tilnærming til styring av tredjepartsrisiko inkluderer også utvikling av planer for en kontrollert avslutning av leverandørsamarbeidet. Dette reduserer risikoen for forstyrrelser og sikrer en smidig overgang ved eventuelle endringer.

Denne tilnærmingen legger grunnlaget for god håndtering av IKT-leverandører og bidrar til økt robusthet og tillit i virksomhetens eksterne relasjoner. Videre i veilederen vil konkrete tiltak og verktøy bli presentert for å støtte arbeidet med helhetlig tredjepartsrisikostyring.

For mer informasjon, se: DORA, kapittel 2, artikkel 11, kapittel 5, artikkel 28, RTS Third-Party ICT Service Policy, artikkel 5, RTS on Risk Management Framework, kapittel 1, artikkel 3 (31) og ITS on Register of Information

4.1. Planlegging

For å sikre en solid grunnmur for et vellykket samarbeid, er det viktig å starte med gode forberedelser i tidlige faser. Dette innebærer blant annet:

- **Identifisering av behov:** Virksomheten bør kartlegge hvilke tjenester eller produkter som er nødvendige. Dette inkluderer å identifisere spesifikke krav til funksjonalitet, ytelse og sikkerhet. For eksempel, om det er behov for spesialiserte IT-løsninger, må virksomheten definere krav til teknologi og datahåndtering.
- **Markedsundersøkelser:** Kartlegging av tilgjengelige IKT-leverandører i markedet gir innsikt i hvilke aktører som kan møte virksomhetens krav. Dette inkluderer å vurdere leverandørens kapasitet, historikk og omdømme.

For mer informasjon, se: DORA, kapittel 5, artikkel 28

4.2. Vurdering og valg av IKT-leverandør

Due diligence er en sentral del av tredjepartsrisikostyring og innebærer en grundig vurdering av IKT-leverandørers egnethet før avtaleinngåelse. Alle leverandører skal vurderes, men det kreves særlig grundighet for IKT-leverandører som understøtter kritiske eller viktige funksjoner, da feil hos disse kan få betydelige konsekvenser for virksomhetens drift.

En vesentlig del av prosessen er å vurdere kritikaliteten på leveransen til IKT-leverandøren. Dette starter med en vurdering av forretningsprosessenes kritikalitet (BIA), etterfulgt av en vurdering av hvor avgjørende leveransen er innenfor denne prosessen. Dette danner grunnlaget for hvordan leverandørens leveranse kategoriseres. En leverandør kan understøtte både kritiske og ikke-kritiske prosesser for samme virksomhet.

Deretter gjennomføres en risikovurdering for å identifisere og håndtere risikoer som finansiell stabilitet, informasjonssikkerhet og regulatoriske krav.

Ved å kombinere disse vurderingene sikres et godt grunnlag for å velge IKT-leverandører som bidrar til trygg og stabil drift gjennom hele samarbeidet.

4.2.1. Vurdering av kritikaliteten på leveransen til IKT-leverandøren

Det er en forutsetning at virksomheten har gjennomført en forretningskonsekvensanalyse (BIA) av sine forretningsprosesser og tjenester for å bruke veilederen for vurdering av IKT-leverandørens kritikalitet.

Denne veilederen gir trinnvise instruksjoner for hvordan matrisen kan benyttes til å vurdere kritikaliteten på leveransen til IKT-leverandøren inn mot de ulike forretningsprosessene i virksomheten. Matrisen er basert på definerte kriterier som vurderes individuelt, scores på en skala fra 1 til 5, og vektes i den samlede vurderingen. En detaljert oversikt over kriteriene og tilhørende vekting finnes i vedlegg 8.3 og tilhørende dokumentet "Standardkriterier for vurdering av kritikaliteten på leveransen til IKT-leverandøren".

Steg 1: Identifiser kriteriene
Begynn med å gjennomgå listen over standardkriterier i matrisen. Disse inkluderer spørsmål som:

- **Kritikalitet** – Er denne IKT-tjenesten ansett som essensiell for forretningsprosesser klassifisert som kritisk/viktig ifølge forretningskonsekvensanalysen (BIA)?

- **Avhengighet** – Hvor avhengig er virksomheten av IKT-tjenesten som leverandøren tilbyr for at den kritiske/viktige funksjonen skal være tilgjengelig?

Forskjellen mellom **kritikalitet** og **avhengighet** ligger i perspektivet og vurderingsfokuset:

- **Kritikalitet** vurderer **hvor viktig** en IKT-tjeneste er i seg selv, basert på om den støtter kritiske eller viktige forretningsprosesser (som identifisert i forretningskonsekvensanalysen). Med andre ord: *Er denne tjenesten kritisk for virksomheten?*
- **Avhengighet** ser på **i hvilken grad** virksomheten faktisk er avhengig av denne IKT-tjenesten for at den kritiske / viktige funksjonen skal kunne fungere. Det betyr at en tjeneste kan være kritisk / viktig, men virksomheten kan ha redundans eller alternative løsninger som reduserer avhengigheten.

Et praktisk eksempel:

La oss si at en bank har en kritisk forretningsprosess for betalingsformidling:

- En bestemt betalingsplattform kan være klassifisert som **kritisk** (kritikalitet) fordi den støtter denne prosessen.
- Samtidig kan bankens **avhengighet** av denne plattformen variere. Hvis banken har en alternativ løsning, er avhengigheten lavere. Hvis det ikke finnes andre alternativer, er avhengigheten høy.

Så, kritikalitet handler om hvor viktig en tjeneste er, mens avhengighet handler om hvor stor påvirkning det har om tjenesten feiler.

Steg 2: Gi en score for hvert kriterium

Bruk en skala fra 1 til 5 for å evaluere hver IKT-leverandør basert på hvert kriterium.

Steg 3: Ta hensyn til vekting

Avhengig av tjenesten og leveransene som underbygger den, kan ulik vekting mellom avhengighet og kritikalitet være nødvendig. Vi foreslår en skjønnsmessig vurdering mellom 40-60 % for å reflektere prioriteringen av kriteriene i den samlede vurderingen.

Steg 4: Tolkning ved hjelp av matrisen

Når den totale kritikalitetsscoren er beregnet, kan IKT-leverandøren plasseres i en av tre kategorier i matrisen:

- **Ikke-kritisk/viktig IKT-leverandør (grønn sone):** Total score: 1 - 3
- **IKT-leverandør av betydning (gul sone):** Total score: 3 - 4
- **Kritisk/viktig IKT-leverandør (rød sone):** Total score 4 - 5

Hvis scoren ligger på skjæringspunktet, for eksempel 4, bør det foretas en skjønnsmessig vurdering av om IKT-leverandøren skal kategoriseres som betydningsfull eller kritisk/viktig. Dette hjelper brukeren med å prioritere oppfølging og risikohåndtering.

Steg 5: Handling basert på resultater
Avhengig av hvilken kritikalitetskategori IKT-leverandøren faller i, bør ulike tiltak vurderes.

- **IKT-leverandører med lav kritikalitet**
    - Årlig oppfølging av leverandør og avtaler.
- **IKT-leverandører av betydning**
    - Kvartalsvis oppfølging av leverandør og avtaler.
    - Vurder behov for etablering av exit-plan.
    - Vurder gjennomgang av tredjepartsattestasjoner.
- **Kritisk/viktige IKT-leverandører**
    - Jevnlig oppfølging av leverandører og avtaler, samt årlig gjennomgang av tredjepartsattestasjoner.
    - Implementer risikoreduserende tiltak.
    - Identifiser alternative leverandører.
    - Etabler tettere samarbeid med leverandøren.
    - Utarbeid en exit-plan.

4.2.2. Risikovurdering av IKT-leverandører

Ved valg av IKT-leverandører bør vurderingen baseres på objektive kriterier for å sikre en rettferdig og konsistent prosess, samtidig som risikoen for subjektive beslutninger reduseres. En standard sjekkliste er et effektivt verktøy for å systematisere evalueringen og dekke sentrale risikoområder, som er nødvendige for å sikre at leverandøren kan møte både nåværende og fremtidige behov.

Som en del av due diligence prosessen må virksomheten gjennomføre en risikovurdering for å identifisere potensielle utfordringer og veie risiko opp mot fordeler. Dette inkluderer vurdering av faktorer som IKT-leverandørens finansielle stabilitet, informasjonssikkerhet, operasjonell kapasitet, overholdelse av regulatoriske

krav, geografisk plassering, enkelhet å bytte, avhengighet av underleverandører og evne til å håndtere endringer eller kriser. Risikovurderingen gir virksomheten verdifull innsikt i hvilke risikoreduserende tiltak som bør iverksettes og sikrer effektiv prioritering av ressurser der risikoeksponeringen er størst. Eksempelvis, dersom det er vanskelig å bytte en IKT-leverandør, kan relevante risikoreduserende tiltak være hyppigere oppfølging av leverandøren og utarbeidelse av en exitplan.

En helhetlig risikovurdering i tidlig fase er avgjørende for å sikre at valg av IKT-leverandør er basert på både kapasitet og stabilitet på lang sikt. Se vedlegg 8.4 for en utarbeidet sjekkliste for IKT-leverandørvurdering.

Vedlegg	Innhold
8.3	Veileder for vurdering av IKT-leverandørens kritikalitet
8.4	Sjekkliste for IKT-leverandørvurdering

For mer informasjon, se: DORA, kapittel 5, artikkel 31

4.3. Avtaleinngåelse og oppstartsfase

Avtaleinngåelse- og oppstartsfasen er en kritisk del av tredjepartsrisikostyringen, hvor virksomheten formaliserer samarbeidet med IKT-leverandøren gjennom juridisk bindende avtaler og implementerer prosesser for integrasjon. Denne fasen gir en mulighet til å fastsette klare forventninger, ansvar og sikkerhetskrav som sikrer at samarbeidet og tredjepartens leveranser er i tråd med kravene i DORA-regelverket.

Gjennom veldefinerte kontrakter og strukturerte prosedyrer for etablering av tjenesten kan virksomheten sikre at IKT-leverandøren oppfyller nødvendige krav knyttet til operasjonell motstandskraft, datasikkerhet og risikostyring. Oppstartsfasen legger også grunnlaget for effektiv overvåking og samarbeid gjennom hele leverandørrelasjonens varighet. Hovedmålet er å minimere risiko ved oppstarten av samarbeidet og å etablere en robust ramme for fremtidige aktiviteter.

4.3.1. Standardiserte maler for kontrakter og vedlegg

Standardiserte kontraktsmaler skal inkludere spesifikke sikkerhetskrav i samsvar med DORA, som dekker datasikkerhet, personvern, tilgangskontroll og hendelseshåndtering. IKT-leverandører skal gi nødvendige opplysninger om bruk av eventuelle underleverandører og deres tjenester. I tillegg bør det defineres klare prosedyrer for endringshåndtering, som inkluderer kommunikasjon, implementering og tilpasning til lovendringer.

Ved inngåelse av avtale med IKT-leverandører som støtter kritiske eller viktige funksjoner, skal kontrakten oppfylle de særskilte kravene i henhold til artikkel 30 (3) i DORA. Dette innebærer blant annet mer omfattende due diligence-prosesser, tiltak for å sikre kontinuitet i kritiske tjenester, samt krav til overvåking, rapportering og risikostyring.

Avtalen skal videre spesifisere krav til regelmessig rapportering og revisjon, inkludert bruk av attestasjonstandarder som ISAE 3000, ISAE 3402, SOC1- eller SOC2-rapporter, for å sikre etterlevelse av sikkerhetsstandarder. Krav om beredskaps- og kontinuitetsplaner må inkluderes for å sikre opprettholdelse av tjenesteleveranser under krisesituasjoner.

Det skal også beskrives sanksjoner ved manglende etterlevelse av avtalte krav, samt kriterier for kontraktens avslutning, herunder dataoverføring og oppsigelsestid. Ansvarsområder for sikkerhet og drift må være tydelig definert. Se vedlegg 8.5 for hvilke krav som bør inkluderes i kontrakt og vedlegg med IKT-leverandører.

4.3.2. Sjekkliste for IKT-leverandøravtaler

Denne sjekklisten er utviklet for situasjoner der IKT-leverandører stiller spesifikke krav, eller der det ikke er hensiktsmessig å benytte egne standardiserte maler (jf. 4.3.1). Formålet med sjekklisten er å etablere et minimumsnivå av sikkerhet og kontroll ved å tydelig definere hvilke elementer som bør være inkludert i avtalen med leverandøren. Se vedlegg 8.6 for utarbeidet sjekkliste for IKT-leverandøravtaler.

Vedlegg	**Innhold**
8.5	Innhold til kontraktsmal og vedlegg
8.6	Sjekkliste for IKT-leverandøravtaler

For mer informasjon, se: DORA, kapittel 5, artikkel 30

4.4. Kontinuerlig oppfølging og overvåking

Virksomheter må implementere robuste mekanismer for å innhente data og dokumentasjon fra IKT-leverandørene, inkludert rapporter om samsvar med sikkerhets- og driftskrav. Oppfølgingen bør være dynamisk og risikobasert, med spesielt fokus på kritiske og viktige IKT-leverandører som leverer kritiske eller viktige tjenester for virksomheten.

Hovedformålet med denne fasen er å opprettholde en proaktiv risikostyring og sikre at eventuelle avvik håndteres raskt og effektivt, noe som bidrar til å styrke den operasjonelle motstandskraften.

4.4.1. Sjekkliste for oppfølging av IKT-leverandører

Kontinuerlig oppfølgning av IKT-leverandører kan sees i tre ulike dimensjoner: Strategisk, taktisk og operasjonelt. Dimensjonene har sine egne formål og virkning, som sammen sikrer en helhetlig styring og kontroll av leverandørrelasjonene. De tre dimensjonene kan forklares slik:

- **Strategisk dimensjon:** Fokuserer på langsiktige mål og strategier. Her handler det om å sikre at IKT-leverandørene støtter virksomhetens overordnede mål og gir forutsigbarhet i leveransene.
    - Gjennomføres av ledelsen mellom selskapene.
- **Taktisk dimensjon:** Handler om å styre og kontrollere leveransene i henhold til avtalte rammer og krav. Dette nivået sikrer at IKT-leverandørene tilpasser seg virksomhetens endrede behov og opprettholder sikkerhetsstandarder.
    - Oppfølgning av avtalt SLA, gjennomganger av risikobildet og for å gjøre løpende tilpasninger til avtalen hvis det anses nødvendig.
- **Operasjonell dimensjon:** Konsentrerer seg om den daglige oppfølgingen av leveransene. Her er målet å sikre at tjenestene leveres som avtalt, og at eventuelle avvik håndteres raskt og effektivt.
    - “Daglig” oppfølgning for å påse at leveransen er i tråd med avtalte forpliktelser.

DORA stiller mer omfattende og tydelige krav til oppfølgingen enn hva som har fulgt av IKT-forskriften, og av hva som foretak skal sikre av IKT-leverandørene sine. De tre dimensjonene for oppfølgning vil være like relevant for oppfølgning under DORA, og kan hjelpe med forståelse for hvordan effektivt gjennomføre denne oppfølgingen.

I vedlegg 8.7 er det laget en sjekkliste for hva IKT-leverandører skal ha på plass i sine selskaper. Dette er på et overordnet nivå, og virksomheten må selv vurdere hvilken detaljgrad som skal benyttes ved kravstilling og oppfølging av hver enkelt IKT-leverandør. Denne beslutningen burde tas med utgangspunkt i kritikalitets- og viktighetsvurderingene etablert under gjennomføring av BIA.

4.4.2. Oppfølgning av uavhengige vurderinger

Som en del av den kontinuerlige oppfølgingen av leverandører i finansbransjen, kan det være nødvendig å innhente og vurdere uavhengige bekreftelser av internkontrollen. For kritiske og viktige leverandører bør uavhengige vurderinger være en del av den årlige oppfølgingen av leverandører.

Formålet med uavhengige vurderinger er å gi en uavhengig vurdering av hvorvidt informasjonssystemene oppfyller spesifikke sikkerhetsstandarder og krav. Uavhengige vurderinger hjelper med å bekrefte at systemene beskytter konfidensialitet, integritet og tilgjengelighet av data, samtidig som de identifiserer og evaluerer potensielle sikkerhetsrisikoer og sårbarheter. Videre sikrer de at organisasjonen overholder relevante lover, forskrifter og standarder, og gir anbefalinger til forbedringer i sikkerhetsprosedyrer og kontroller. Dette bidrar til å bygge tillit hos kunder, partnere og interessenter ved å demonstrere en forpliktelse til sikkerhet og digital motstandskraft.

Uavhengige vurderinger bør inkludere en vurdering av de tjenestene som leveres til din virksomhet, inkludert sikkerhet, personvern og finansiell kontroll. Deretter bør man sikre at de har uavhengige kontroller som er relevante for spesifikke prosesser og leveranser.

Generelt, hvis rapportene inneholder avvik eller hvis kontrollene ikke oppfyller kravene, må behovet for ytterligere tiltak vurderes. Dette innebærer å analysere leverandørens forklaring på avvikene og deres plan for oppfølging. I tilfeller der det er usikkerhet om tiltakene er tilstrekkelige, bør alternative handlinger vurderes, som ytterligere testing av leverandørens kontroller.

4.4.3. Informasjonsdeling – cyber- og andre relevante hendelser

Dersom virksomhetene i finansnæringen støtter opp om Nordic Financial CERT (NFCERT) som delingsplattform for sikkerhetsrelatert informasjon, vil det styrke informasjonsdeling og læring i bransjen som helhet.

Virksomheter bør oppfordre IKT-leverandører til å være åpne om sikkerhetsrelaterte hendelser, men respektere behovet for å beskytte sensitiv informasjon inntil sårbarheter er lukket og hendelser håndtert. NFCERT har prosedyre for å dele informasjon anonymt med bransjen, så IKT-leverandører kan på generelt grunnlag oppfordres til å dele direkte med NFCERT.

Vedlegg	Innhold
8.7	Sjekkliste for oppfølging av IKT-leverandører

For mer informasjon, se: DORA, kapittel 2, artikkel 5 - 16

4.5. Exitstrategi og avslutning av samarbeid

Utarbeidelse av exitstrategier for kritiske og viktige IKT-leverandører er en viktig del av tredjepartsrisikostyringen. En god exitstrategi sikrer en kontrollert og strukturert avslutning av samarbeidet med IKT-leverandøren. Exitstrategien omfatter både planlegging for avtalt avslutning og håndtering av ekstraordinære situasjoner hvor samarbeidet må termineres raskt.

Det er avgjørende å ha alternative IKT-leverandører tilgjengelig for å sikre kontinuitet i tjenesteleveransen. I tråd med DORA bør en exitstrategi være rettet mot å redusere risikoen for operasjonelle forstyrrelser, ivareta sikker håndtering av data og opprettholde samsvar med regulatoriske krav. Dette er særlig kritisk for virksomhetens kjerneprosesser, der avhengigheten til én enkelt IKT-leverandør kan utgjøre en betydelig risiko. Eksempler på slike risikoer inkluderer leverandørens konkurs, oppkjøp av uønskede aktører, dårlig leveransekvalitet eller avvik mellom kontrakt og leveranse. En systematisk vurdering av alternative IKT-leverandører er derfor nødvendig for å sikre robusthet og operasjonell fleksibilitet.

Avslutning av samarbeid med en IKT-leverandør eller underleverandør krever en grundig tilnærming for å unngå uforutsette konsekvenser. Dette innebærer:

- **Kommunikasjon:** Tidlig og tydelig kommunikasjon med IKT-leverandøren om årsaken til avslutningen og nødvendige steg videre.
- **Datasanering:** Sørge for at all informasjon som har blitt delt med IKT-leverandøren blir returnert eller destruert på en sikker måte.
- **Overføring av tjenester:** Planlegging av hvordan kritiske funksjoner kan videreføres, enten internt eller via en ny IKT-leverandør.
- **Evaluering og dokumentasjon:** Gjennomgang av hele samarbeidet for å lære av prosessen og dokumentere viktige erfaringer.

En god exitstrategi omfatter tydelige prosesser for tilbakeføring eller destruksjon av data, vurdering av alternativer for kritiske tjenester, og grundig dokumentasjon av alle aktiviteter knyttet til termineringen. Hovedmålet er å sikre at virksomheten opprettholder operasjonell stabilitet, selv etter avslutning av et leverandørsamarbeid.

4.5.1. Exitstrategi og sjekkliste for exitplan

Exitstrategi vs. Exitplan

- **Exitstrategi:** En overordnet plan for avslutning av samarbeid med en IKT-leverandør, som dekker virksomhetens interne prosesser frem til en beslutning om exit er tatt. Strategien har som mål å minimere risiko og sikre kontinuitet, inkludert håndtering av data og kritiske tjenester.
- **Exitplan:** En detaljert plan som trer i kraft når beslutning om exit er tatt. Planen involverer IKT-leverandøren i prosessen og beskriver stegene for overgangsperioder, risikohåndtering og databehandling, slik at stabil drift opprettholdes under og etter avslutningen.

DORA stiller tydelige krav til innhold og betraktninger som skal ha blitt vurdert i en exitstrategi. Strategien må planlegge for ulike typer exit-scenarier, som inkluderer både planlagte avslutninger av leverandørforhold og ekstraordinære avslutninger. Sistnevnte kan oppstå når en kritisk eller viktig IKT-leverandør ikke oppfyller sine forpliktelser, eller når IKT-leverandøren forhindrer virksomheten i å oppfylle sine regulatoriske plikter. En god exitstrategi bør utarbeides og forankres tidlig i leverandørforholdet, slik at virksomheten er godt forberedt på å håndtere avslutningen på en kontrollert og trygg måte.

For å sikre en vellykket gjennomføring av en exitstrategi, er det avgjørende å ha en detaljert exitplan på plass. Denne planen bør beskrive de praktiske stegene for implementeringen, og inkluderer prosedyrer for håndtering av data, overføring av kritiske tjenester og risikohåndtering. I tråd med DORA gjelder proporsjonalitetsprinsippet også for utarbeidelsen av exitplaner. Det betyr at planen skal tilpasses virksomhetens størrelse, kompleksitet og risikonivå, slik at den er både praktisk og effektiv i ulike scenarioer.

Ved terminering av kontraktsforholdet skal exitplanene ha som mål å minimere negativ påvirkning på driften til virksomheten og dens kunder. Planene må derfor sikre at driften kan opprettholdes på en forsvarlig måte i overgangsperioden.

For å støtte utarbeidelsen av exitplanene, er det laget en oversikt over hva de bør inneholde, samt en sjekkliste for å påse at de viktigste temaene i DORA er vurdert i planverket. Denne informasjonen finnes i vedlegg 8.8. Dette er ikke uttømmende lister, og ytterligere vurderinger kan være nødvendige.

Sjekkliste for exitplaner:

For å sikre grundig utarbeidelse av exitplaner, er det laget en sjekkliste med viktige vurderinger som bør inkluderes. Sjekklisten dekker sannsynligvis ikke alle krav eller detaljer som skal være med i en fullstendig exitplan, men dens hovedformål er å sikre at de viktigste momentene i DORA er vurdert. Hvis svaret på noen spørsmål er «nei»,

bør dette enten behandles som et separat punkt eller forklares hvorfor det ikke er vurdert. Se vedlegg 8.9 for sjekklisten.

Revisjon og testing av exitplaner:

DORA krever at exitplaner regelmessig testes, gjennomgås og revideres for å sikre at de forblir effektive og oppdaterte. Et årshjul kan være nyttig for å planlegge disse aktivitetene. I vedlegg 8.10 finner du punktene som bør vurderes ved en gjennomgang av planene.

For å kunne gjennomføre regelmessig og realistisk testing, må exitplanene utarbeides på en måte som gjør dem testbare. Det stilles ikke krav om at testene må gjennomføres i en faktisk driftskontekst. I henhold til RTS for Third-Party ICT Service Policy kan testene gjennomføres som bordøvelser, skrivebordsøvelser eller andre type øvelser, men de må baseres på plausible scenarier og realistiske hendelser. Hvordan virksomheten velger å teste sine planer, bør vurderes ut fra hva som anses som den mest hensiktsmessige og nyttige øvelsen.

DORA stiller også krav om at exitplanene skal være testet tilstrekkelig. Hva som defineres som tilstrekkelig, må vurderes i lys av DORAs prinsipp om proporsjonalitet. En testplan bør derfor utarbeides med hensyn til sannsynligheten for at en plan må iverksettes, samt de scenariene som kan inntreffe. Scenarier med høyere sannsynlighet for å inntreffe eller med større påvirkning på kritiske og viktige forretningsfunksjoner bør testes hyppigere. Erfaringene som innhentes gjennom testing, bør benyttes til revisjon av exitplanene. Vedlegg 8.11 gir tips til revisjon av exitplaner.

Tidshorisont av exitplan

Ved utarbeidelse av exitplanen må tidshorisonten for planen vurderes. Denne skal være realistisk og proporsjonal med tjenesten som leveres, den forretningsmessige funksjonen den understøtter og bakgrunnen for at en exit er besluttet. Hvis det ikke finnes alternative IKT-leverandører på kort sikt, vil en lengre tidshorisont være nødvendig. Exitplanen må da sikre kontinuitet i tjenesten frem til et leverandørbytte, eller en plan for avvikling av tjenesten. For noen sentrale aktører som ikke lett kan byttes ut i Norden, kan en langsiktig exitplan inkludere vurdering av alternative IKT-leverandører i Europa.

Det skjønnsbaserte proporsjonalitetsprinsippet vil være sentralt når tidshorisonten vurderes. Dette vil baseres på faktorer som når exit kan gjennomføres, mulighet for leverandørbytte eller intern flytting, hvor kritisk eller viktig tjenesten er, samt størrelsen på leveransen som støtter en viktig eller kritisk forretningsfunksjon.

Vedlegg	Innhold
8.8	Innhold til exitplan
8.9	Sjekkliste for exitplan
8.10	Triggere for exitplan
8.11	Revisjon av exitplan

For mer informasjon, se: DORA, kapittel 1, artikkel 4, kapittel 5, artikkel 28, 30 og RTS Third-Party ICT Service Policy, artikkel 10

5. Ordliste

- **Avtaleinngåelse**: Prosessen med å inngå en formell avtale eller kontrakt med en tredjepartsleverandør.
- **BIA (Business Impact Analysis):** En analyseprosess for å identifisere kritiske forretningsfunksjoner og vurdere konsekvensene av avbrudd.
- **Datahåndtering:** Prosessen med å administrere data gjennom hele livssyklusen.
- **DORA**: Digital Operational Resilience Act
- **Due diligence:** En grundig vurdering og analyse av potensielle IKT-leverandører for å sikre at de oppfyller nødvendige standarder og krav.
- **Endringshåndtering:** Prosessen med å administrere endringer i systemer og prosesser.
- **Exit-strategi:** Plan for avslutning av samarbeid med leverandører.
- **Forretningsprosess:** refererer til en helhetlig serie av aktiviteter som er nødvendig for å sikre en effektiv drift og levering av finansielle tjenester. Dette inkluderer typiske prosesser som lånebehandling, risikovurdering og transaksjonshåndtering.
- **Identitets- og tilgangsstyring (IAM):** System for å administrere brukertilgang til ressurser.
- **IKT-tjenester:** Digitale og datadrevne tjenester som leveres gjennom IKT-systemer til én eller flere interne eller eksterne brukere på en kontinuerlig basis.
- **Konsentrasjonsrisiko:** Risiko knyttet til avhengighet av en enkelt leverandør.
- **Kontinuitetsplan**: Plan for å sikre opprettholdelse av ulike prosseser under forstyrrelser.
- **Kontrolltiltak:** Tiltak for å redusere eller eliminere risiko.
- **Kritikalitetsvurdering**: Evaluering av hvor viktig en IKT-leverandør eller tjeneste er for virksomhetens operasjonelle stabilitet.
- **Kritisk/viktig funksjon:** En rekke spesifikke oppgaver eller aktiviteter som er viktig for en finansinstitusjons forretningsprosesser. Forstyrrelser i denne funksjonen kan påvirke institusjonens økonomiske ytelse, tjenestestabilitet eller evne til å oppfylle lovpålagte forpliktelser.
- **Leverandøravhengighet**: Graden av en virksomhets avhengighet av en IKT-leverandør for å opprettholde kritiske funksjoner.
- **Leverandørkjede**: Nettverk av leverandører som bidrar til en virksomhets tjenester.
- **Leverandørstyring**: Overvåking og administrasjon av forholdet og ytelsen til IKT-leverandører
- **Operasjonell motstandskraft**: Evnen til en virksomhet å opprettholde kritiske funksjoner under og etter en forstyrrelse.
- **Oppstartsfasen**: Integreringsprosessen hvor en ny IKT-leverandør blir formelt innlemmet i virksomhetens systemer og prosesser.
- **Risikostyring:** Prosessen med å identifisere, vurdere og redusere risiko.
- **Risikoprofil:** Samlet vurdering av risikoer knyttet til en virksomhet eller prosess.

- **Risikovurdering**: Prosessen med å identifisere, analysere og evaluere risikoer for å minimere deres potensielle påvirkning.
- **RTO/RPO/MTPD:** Gjenopprettingstid, gjenopprettingspunkt og maksimal tolerabel nedetid.
- **SLA (Service Level Agreement)**: Avtale som definerer tjenestenivåer mellom leverandør og kunde.
- **Skyavhengigheter:** Avhengighet av skybaserte tjenester i leverandørkjeden.
- **Tredjepartsattestasjoner:** Dokumentasjon fra tredjepart som bekrefter overholdelse av standarder.
- **Tredjepart** En ekstern enhet eller organisasjon som leverer tjenester eller produkter til en virksomhet, men som ikke er en del av virksomheten selv.
    - **Tredjepartsrisiko**: Risikoen for at en ekstern IKT-leverandør kan påvirke en virksomhets operasjonelle stabilitet, sikkerhet eller samsvar med regelverk.
    - **Tredjepartsrelasjoner**: Forholdet mellom en virksomhet og dens eksterne IKT-leverandører eller partnere.
    - **Tredjepartsutvelgelse**: Prosessen med å identifisere og velge passende IKT-leverandører basert på spesifikke kriterier og behov.
- **Underleverandør:** En leverandør som leverer tjenester til en hovedleverandør.

6. Litteraturliste

Bank for International Settlements. (2024, Juli). *Principles for the sound management of third-party risk*. Hentet fra Basel Committee on Banking Supervision: https://www.bis.org/bcbs/publ/d577.pdf

European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union. (2024, November 29). *Implementing regulation - EU - 2024/2956 - EN - EUR-Lex*. Hentet fra Eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32024R2956&qid=1739720633558

European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union. (2024, Juni 25). *RTS ICT RIsk Management Framework*. Hentet fra EUR-lex.eu: https://eur-lex.europa.eu/eli/reg_del/2024/1774/

European Parliament, Council of the European Union. (2022, Desember 14). *Regulation - 2022/2554 - EN - DORA - EUR-Lex*. Hentet fra EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN#d1e2178-1-1

European Supervisory Authorities (EBA, ESMA and EIOPA). (2024, Juli 26). *Final report DORA RTS on subcontracting*. Hentet fra Eba.europa.eu: https://www.eba.europa.eu/sites/default/files/2024-07/f724684d-74c8-4f7d-a467-3df456c73b26/JC%202024-53_Final%20report%20DORA%20RTS%20on%20subcontracting.pdf

European Supervisory Authorities (EBA, ESMA and EIOPA). (2024, Januar 10). *Final report on Draft Regulatory Technical Standards Third-Party ICT Service Policy*. Hentet fra EBA Europa: https://www.eba.europa.eu/sites/default/files/2024-01/88355b09-d6e6-4d39-a3e6-c710549cc717/JC%202023%2084%20-%20Final%20report%20on%20draft%20RTS%20to%20specify%20the%20policy%20on%20ICT%20services%20supporting%20critical%20or%20important%20functions.pdf

Financial Stability Board. (2023, Desember 4). *Enhancing Third-Party Risk Management and Oversight*. Hentet fra FSB.org: https://www.fsb.org/uploads/P041223-1.pdf

Finansdepartementet. (2024, Januar 23). *Nytt regelverk for digital operasjonell - Norsk gjennomføring av Digital Operational Resilience Act (DORA)*. Hentet fra Regjeringen.no: https://www.regjeringen.no/contentassets/2ff78f76943c475492b9641755222210/horingsnotat.pdf

Finanstilsynet. (2019, Desember 18). *Rapportering av IKT-hendelser til Kredittilsynet*. Hentet fra Finanstilsynet.no: https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2009/rapportering-av-ikt-hendelser-til-kredittilsynet/

Finanstilsynet. (2024, September 16). *Finanstilsynet*. Hentet fra Risiko- og sårbarhetsanalyse (ROS) 2024: https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/2024/ros-2024/risiko--og-sarbarhetsanalyse-ros-2024/

Forum for informasjonssikkerhet i kraftforsyningen. (2024, August). *Veileder for sikkerhet i anskaffelser og leverandørkjeder*. Hentet fra FSK-forum.no: https://fsk-forum.no/wp-content/uploads/2023/08/FSK-Veileder-for-sikkerhet-i-anskaffelser-og-leverandorkjeder-Endelig-versjon-august-2023.pdf

NVE. (2020, Januar). *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen*. Hentet fra NVE.no: https://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf

7. Ansvar ved bruk av veilederen

Denne veilederen er utarbeidet av Finans Norge for sine medlemmer, med mål om å gi innsikt i styring av IKT-tredjepartsrisiko i finansnæringen. Dokumentet er utformet for å hjelpe virksomheter med å forstå og håndtere komplekse risikostyringsprosesser knyttet til IKT-leverandører.

Innholdet bygger på beste praksis og gjeldende kunnskap ved utgivelsestidspunktet, men er ikke ment å være uttømmende eller spesialtilpasset individuelle behov. Veilederen bør ikke erstatte profesjonell rådgivning eller brukes som eneste grunnlag for kritiske beslutninger uten ytterligere konsultasjon. Den pålegger ikke Finans Norges medlemmer spesifikke plikter eller forbud. Selv om veilederen refererer til ulike kilder, tar Finans Norge ikke ansvar for deres nøyaktighet eller oppdatering.

Veilederen er et levende dokument og ikke et sluttprodukt. Finans Norge og dets medlemmer planlegger å revidere den ved behov. Finans Norge påtar seg ikke ansvar for eventuelle feil, mangler eller konsekvenser som følge av bruk av informasjonen i veilederen. Brukere oppfordres til å søke råd fra kvalifiserte fagpersoner for å sikre at alle aspekter av tredjepartsrisiko blir tilstrekkelig vurdert og håndtert i henhold til deres spesifikke situasjon.

Lover, forskrifter og standarder kan endres over tid, så det er viktig å holde seg oppdatert på gjeldende regelverk. Finans Norge fraskriver seg ansvar for oppdatering av innholdet etter publisering.

Veilederen illustrerer hva norsk finansnæring kan oppnå gjennom godt samarbeid. Finans Norge ønsker å takke alle som har bidratt til arbeidet med veilederen og ser frem til et fortsatt samarbeid i forbindelse med videreutvikling og oppdatering av denne.

For ytterligere informasjon eller spesifikke råd, anbefales det å kontakte en profesjonell rådgiver.

8. Vedlegg

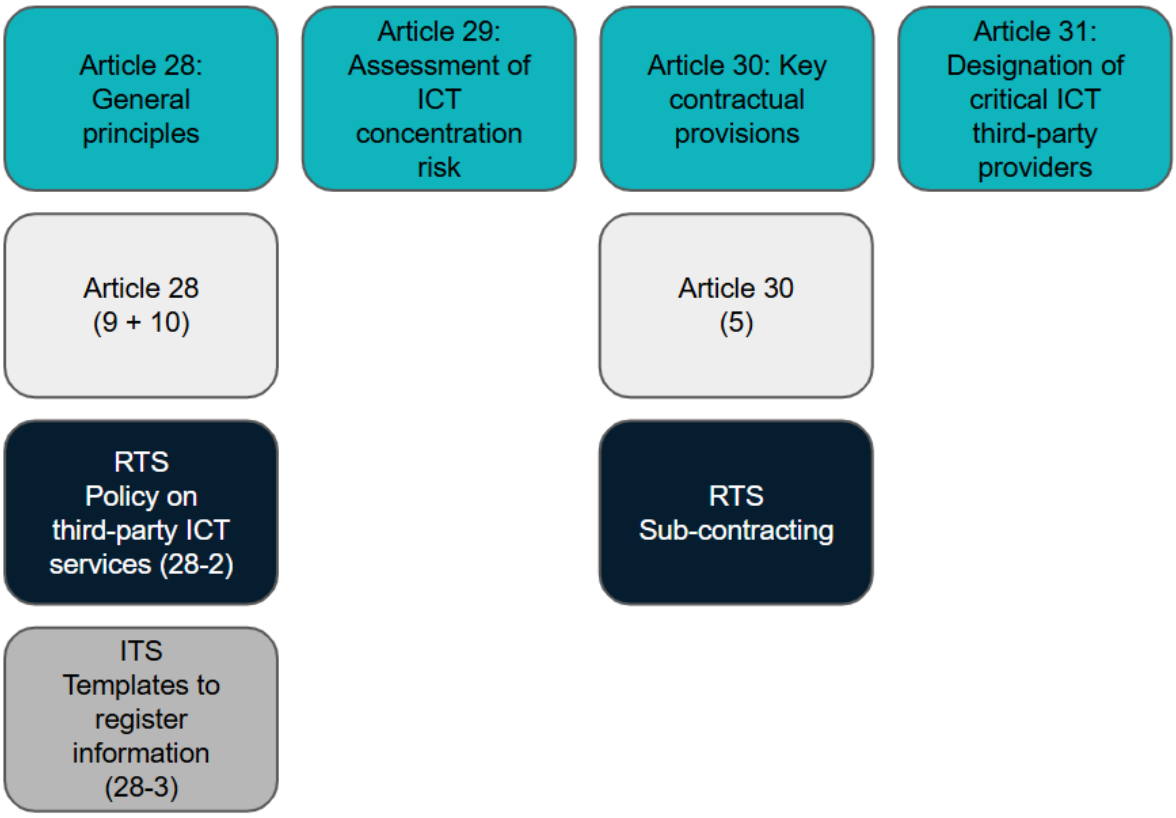
8.1. Sammenheng mellom DORA og standarder

Dora (5) -Third party risk - Article 28-44

RTS: 2023 84 Policy on ICT services performed by a third party (article 28), Subcontracting (article 30)

ITS: Templates to register information

GL: Cooperation between European Supervisory Authorities (ESAs) and competent authorities (Cas) regarding the structure of the oversight (article 32)



8.2. Ressurspersoner

I arbeidet med veilederen har Finans Norge hatt kontakt med ressurspersoner i finansnæringen. Vi retter en stor takk til alle gode bidragsytere:

Navn	Bedrift
Tom-André Røgden	Sparebank1 Utvikling
Espen Jul Larsen	Gjensidige
Herman Vidje	Storebrand
Trygve Dahl	Storebrand
Lars Ivar K. Kittelsaa	Sparebanken Vest
Hilde Seem	KLP
Ine Ljosland Strand	DNB
Steinar Lieungh	Fremtind
Tore Ingholm	Lokalbank
Stein Gytre	Lokalbank
Are Henrik Farstad	Eika Gruppen
Gaute Loftesnes	Eika Gruppen
Pål Christian Waag	Finans Norge
Lars Erik Fjørtoft	PwC
Ludvig-Johannes H. Carlsen	PwC
Eirik Strømmen Engum	PwC

8.3. Veileder for vurdering av kritikaliteten på leveransen til IKT-leverandøren (4.2.1)

Denne veilederen gir trinnvise instruksjoner for hvordan matrisen kan benyttes til å vurdere kritikaliteten på leveransen til IKT-leverandøren inn mot de ulike forretningsprosessene i virksomheten. *Det er en forutsetning at virksomheten har gjennomført en forretningskonsekvensanalyse (BIA) av sine forretningsprosesser og tjenester for å bruke denne metoden.*

Matrisen er basert på definerte kriterier som vurderes individuelt, scores på en skala fra 1 til 5, og vektes i den samlede vurderingen. En detaljert oversikt over kriteriene og tilhørende vekting finnes i det tilhørende dokumentet "Standardkriterier for vurdering av kritikaliteten på leveransen til IKT-leverandøren".

Steg 1: Identifiser kriteriene
Begynn med å gjennomgå listen over standardkriterier i matrisen. Disse inkluderer spørsmål som:

- **Kritikalitet** – Er denne IKT-tjenesten ansett som essensiell for forretningsprosesser klassifisert som kritisk/viktig ifølge forretningskonsekvensanalysen (BIA)?
- **Avhengighet** – Hvor avhengig er virksomheten av IKT-tjenesten som leverandøren tilbyr for at den kritiske/viktige funksjonen skal være tilgjengelig?

Steg 2: Gi en score for hvert kriterium
Bruk en skala fra 1 til 5 for å evaluere hver IKT-leverandør basert på hvert kriterium.

Skåringskriterier for kritikalitet (baseres på egen BIA)	Skåringskriterier for avhengighet
1. Kritikalitet er ingen eller ubetydelig.	1. Ingen avhengighet: Det er ingen avhengighet av denne IKT-leveransen
2. Kritikalitet er lav.	2. Lav avhengighet: IKT-leveransen har liten innvirkning og kan enkelt erstattes eller kompenseres for.
3. Kritikalitet er moderat.	3. Moderat avhengighet: IKT-leveransen har en betydelig, men håndterbar innvirkning på systemet eller prosessen.
4. Kritikalitet er høy	4. Høy avhengighet: IKT-leveransen er svært viktig og vanskelig å erstatte, noe som kan skape utfordringer ved fravær eller feil.
5. Kritikalitet er veldig høy	5. Kritisk avhengighet: IKT-leveransen er avgjørende for systemets funksjon, og dens fravær eller svikt vil føre til store konsekvenser.

Steg 3: Ta hensyn til vekting
Avhengig av tjenesten og leveransene som underbygger den, kan ulik vekting mellom avhengighet og kritikalitet være nødvendig. Vi foreslår en skjønnsmessig vurdering mellom 40-60 % for å reflektere prioriteringen av kriteriene i den samlede vurderingen.

Steg 4: Tolkning ved hjelp av matrisen
Når den totale kritikalitetsscoren er beregnet, kan IKT-leverandøren plasseres i en av tre kategorier i matrisen:

- **Ikke-kritisk/viktig IKT-leverandør (grønn sone):** Total score: 1 - 3
- **IKT-leverandør av betydning (gul sone):** Total score: 3 - 4
- **Kritisk/viktig IKT-leverandør (rød sone):** Total score 4 - 5

Hvis scoren ligger på skjæringspunktet, for eksempel 4, bør det foretas en skjønnsmessig vurdering av om IKT-leverandøren skal kategoriseres som betydningsfull eller kritisk/viktig. Dette hjelper brukeren med å prioritere oppfølging og risikohåndtering.

Steg 5: Handling basert på resultater

Avhengig av hvilken kritikalitetskategori leveransen til IKT-leverandøren faller i, bør ulike tiltak vurderes.

Ikke-kritisk/viktig IKT-leverandører	Årlig oppfølging av IKT-leverandør og avtaler.
IKT-leverandører av betydning	Kvartalsvis oppfølging av IKT-leverandør og avtaler. Vurder behov for etablering av exitplan. Vurder gjennomgang av tredjepartsattestasjoner.
Kritisk/viktige IKT-leverandører	Jevnlig oppfølging av leverandører og avtaler, samt årlig gjennomgang av tredjepartsattestasjoner. Tiltak som implementeres for IKT-leverandøren bør være risikoreduserende tiltak, identifisering av alternative IKT-leverandører, tettere samarbeid, utarbeidelse av exit-plan.

8.4. Standard sjekkliste for risikovurdering av IKT-leverandører (4.2.2)

#	Kontrollpunkt	Beskrivelse
1	**Finansielle vurderinger**	Gjennomgå IKT-leverandørens økonomiske rapporter for å vurdere deres stabilitet og levedyktighet
2	**Informasjonssikkerhet**	Kartlegg sikkerhetstiltakene IKT-leverandøren har implementert for å beskytte data og systemer
3	**Tidligere erfaring**	Innhent referanser fra andre kunder for å vurdere IKT-leverandørens pålitelighet og kvalitetsnivå
4	**Enkelhet å bytte**	Hvor enkelt er det å bytte fra en bestemt IKT-leverandør til en annen for dette produktet eller tjenesten?
5	**Underleverandører**	Identifiser om IKT-leverandøren bruker underleverandører, og vurder deres potensielle risiko
6	**Konsentrasjonsrisiko**	Kartlegg antall tjenester eller produkter som allerede er kjøpt fra samme IKT-leverandør, og vurder om leverandørkonsentrasjonen er akseptabel eller om det er behov for diversifisering
7	**Kritisk IKT-leverandør i EU**	Sjekk om IKT-leverandøren er klassifisert som kritisk i henhold til leverandørregisteret som skal opprettes under DORA iht. Register of Information. Vurder hvilke konsekvenser denne klassifiseringen kan ha for din virksomhet.

8.5. Standardiserte maler for kontrakter og vedlegg (4.3.1)

#	Kontrollpunkt	Beskrivelse
1	**Sikkerhetskrav**	Inkluder spesifikke krav til datasikkerhet, personvern, tilgangskontroll og hendelseshåndtering i kontrakten, i tråd med DORA.
2	**Bruk av underleverandører**	Still krav til at IKT-leverandør skal opplyse om hvilke underleverandører de benytter og hvilke tjenester de leverer som er relevant for egen leveranse.
3	**Endringshåndtering**	Definer prosedyrer for håndtering av endringer i tjenestene eller sikkerhetskravene, inkludert hvordan slike endringer skal kommuniseres og implementeres. Avtale må ha rom for vilkårsendringer som følge av endring i lovgivning eller rettspraksis, og virksomheten må faktisk følge opp dette dersom nødvendig.
4	**Rapportering og revisjon**	Etabler krav til regelmessig rapportering og revisjon for å overvåke IKT-leverandørens etterlevelse av attestasjonstandarder og operasjonell motstandskraft, eks. ISAE 3000 med relevant innretning, SOC-rapporter eller tilsvarende standard.
5	**Kontinuitets-planlegging**	Inkluder krav om beredskapsplaner og kontinuitetsplaner for å sikre at tjenestene kan opprettholdes under ulike krisesituasjoner.
6	**Sanksjoner og konsekvenser**	Beskriv sanksjoner eller konsekvenser ved manglende etterlevelse av avtalte krav, for å sikre at IKT-leverandøren tar sine forpliktelser på alvor.
7	**Exitplaner**	Det må etableres kriterier for å gå ut av kontrakten/avbryte samarbeidet med IKT-leverandøren. Avtale hvordan avtalen kan avsluttes, inkludert krav til tilbakeføring av data og oppsigelsestid.
8	**Tydelige ansvarsområder**	Definer hvilken part som har ansvar for ulike deler av tjenesten, inkludert oppfølging av sikkerhet og drift.

8.6. Standard sjekkliste for IKT-leverandøravtaler (4.3.2)

#	Kontrollpunkt	Krav i DORA
1	Rettigheter og forpliktelser mellom partene skal være tydelig definert, skriftlig og tilgjengelig for alle parter. Den skal inneholde nivået.	30.1
2	Er IKT-leverandør å regne som en kritisk eller viktig IKT-leverandør? (Ja/Nei)	-
	Krav til avtaler med alle IKT-leverandører	
3	Inneholder avtalen informasjon om hva som skal leveres?	30.2.a
4	Benytter IKT-leverandøren underleverandører?	30.2.a
5	Inneholder avtalen en beskrivelse av vilkårene for underleverandøren?	30.2.a
6	Beskriver avtalen lokasjonen hvor tjenesten leveres fra?	30.2.b
7	Inkluderer avtalen beskrivelse av hvor data, inkludert personopplysninger, skal lagres og behandles?	30.2.b
8	Inkluderer avtalen beskrivelse av varsling i forkant av planlagte endringer i slike lokasjoner?	30.2.b
9	Inneholder avtalen beskrivelse av hvordan data, inkludert personopplysninger, sikres iht. konfidensialitet, integritet og tilgjengelighet	30.2.c
10	Inneholder avtalen bestemmelser om sikring av adgang, gjenoppretting og tilbakelevering av data, inklusivt personopplysninger i et tilgjengelig format ved avvikling, avbrudd, oppsigelse eller konkurs	30.2.d
11	Beskriver avtalen ulike servicenivåer, revisjoner og oppdatering av disse?	30.2.e
12	Inkluderer avtalen forpliktelser til bistand fra IKT-leverandøren ved IKT-hendelser til avtalt pris, i den grad pris ikke er avtalt er det uten ekstra kostnad?	30.2.f
13	Forplikter IKT-leverandøren seg til å samarbeide fullt ut med kompetente myndigheter eller de selskap/personer virksomheten utnevner?	30.2.g
14	Beskriver avtalen oppsigelsesrett og minimums varslingsperiode for	30.2.h

	terminering av avtalen, som tillater operativ drift iht. myndighetenes krav?	
15	Beskrives IKT-leverandørens vilkår for deltakelse i finansforetakets program- og opplæring for digital motstandsdyktighet?	13.6 30.2 (i)
Krav til avtaler med IKT-leverandører klassifisert som kritiske eller viktige (30.3) *Følgende krav skal kontraktsfestes i avtalen.*		
16	Beskriver avtalen en fullstendig SLA, inkludert oppdateringer og revisjoner, med presise kvalitative og kvantitative ytelsesmål innenfor avtalte tjenestenivå?	30.3.a
17	Beskriver avtalen hvordan krav i SLA-en overvåkes, samt hvordan korrigerende tiltak kan iverksettes uten unødig forsinkelse når avtalte SLA-nivå ikke oppfylles?	30.3.a
18	Beskrives oppsigelsesfrister og rapporteringsfrister fra IKT-leverandøren, samt varsling om enhver utvikling som kan ha vesentlig innvirkning på evnen til å effektivt levere IKT-tjenester som støtter kritiske eller viktige funksjoner i tråd med avtalte SLA-krav?	30.3.b
19	Beskriver avtalen krav om implementering og testing av forretningskontinuitetsplaner, etablering av IKT-sikkerhetstiltak, verktøy og retningslinjer som sikrer et godt nok sikkerhetsnivå for levering av tjenester, i samsvar med gjeldende regulatoriske rammeverk?	30.3.c
20	Beskriver avtalen hvordan IKT-leverandøren skal delta og fullt ut samarbeide med virksomhetens TLPT.	26 27 30.3.d
21	Beskriver avtalen krav til ubegrenset rettighet til tilgang, inspeksjon og revisjon fra virksomheten, tilsynsmyndighet eller oppnevnt tredjepart? Inkl. rett til å ta kopier av relevant dokumentasjon på stedet hvis kritisk for driften.	30.3.e (i)
22	Beskriver avtalen IKT-leverandørens plikt til å samarbeide fullt ut under inspeksjon og revisjoner på stedet?	30.3.e (iii)
23	Inkluderer avtalen IKT-leverandørens plikt til å gi detaljer om omfang, prosedyrer som skal følges og hyppigheten av slike inspeksjoner og revisjoner?	30.3.e (iv)
24	Inkluderer avtalen en beskrivelse av exit-strategi, med særlig fokus på obligatorisk tilstrekkelig overgangsperiode som både kan sikre fortsettelse av leveranse, alternativt mulighet til migrering av løsning til annen IKT-leverandør, eventuelt til interne løsninger hos virksomheten?	30.3.f

8.7. Sjekkliste oppfølgning av IKT-leverandører (4.4.1)

Listen er basert på Finanstilsynet sine egne forslag i ROS-analyse for 2024.

#	Kontrollpunkt	Beskrivelse
1	**Styring og kontroll**	Sikre at det er etablert tilfredsstillende styring og kontroll.
2	**Risikostyring**	Sikre at det er tilfredsstillende risikostyring.
3	**Hendelse/respons**	Sikre at det er etablert et hensiktsmessig regime for å respondere på ulike typer hendelser hos oppdragstaker og dens underleverandører, slik at oppdragsgiver kan rapportere eventuelle rapporteringspliktige hendelser til Finanstilsynet iht. DORA 19 (1) samt dekke forpliktelser i DORA 17 (2).
4	**Kontunitetstesting**	Sikre at foretakets krav til gjenoppretting (RTO/RPO/ MTPD) er ivaretatt og dokumentert i rapporter fra utført beredskaps- og kontinuitetstesting for de kritiske og viktige prosessene.
5	**Sikkerhetstesting**	Sikre at det gjennomføres tilstrekkelige sårbarhets- og penetrasjonstester og andre typer sikkerhetstesting.
6	**IKT-sikkerhetspolicy**	Sikre at kravene i foretakets IKT-sikkerhetspolicy er ivaretatt.
7	**Endrings-håndtering**	Sikre at kvaliteten på endringshåndteringen er ivaretatt. Foretaket bør blant annet ha oversikt over antall feil som følge av endringer.
8	**Risiko- og trusselovervåking**	Sikre at det er etablert betryggende risiko- og trusselovervåking.
9	**Tilgangsstyring**	Sikre at system og rutiner for identitets- og tilgangsstyring (IAM) er etablert.
10	**Logging**	Sikre at den etablerte system- og applikasjonsloggingen har tilstrekkelig omfang og kvalitet.
11	**Eskalering**	Sikre at det er etablert klare rapporteringslinjer og eskaleringsstrukturer for å sikre at regulatoriske krav er ivaretatt.
12	**Attestasjoner**	Få tilsendt ISAE 3000 / 3402 / SOC1 / SOC2 eller tilsvarende standard. Må ha en plan for å følge opp rapporten internt, det er ikke nok å gi den videre til revisor.

* Kravstillelse til IKT-leverandør vil avhenge av deres kritikalitet og/eller viktighet overfor selskapets øvrige forretningsprosesser. Kravstillelse av RTO/RPO/MTPD må settes iht. input fra BIA og vil kunne variere fra leverandør til leverandør.

8.8. Innhold til exitplan (4.5.1)

Overskrift	Beskrivelse
Mål	De viktigste målene med exitstrategien.
Suksess	Viktige suksesskriterier.
Ressurser	Inkludert mennesker, økonomi og teknologi; for å sikre en smidig avslutning og overgang.
Roller og ansvar	Roller og ansvar for å håndtere exit-planen og eventuelle overgangsaktiviteter.
Alternativer	Alternative løsninger og midlertidige tiltak for å støtte en smidig avslutning og overgang.
Utløsere	Inkludert nøkkelprestasjoner og risikokriterier som kan utløse en potensiell exit.
Avhengigheter	Identifikasjon av viktige underleverandører og eventuelle skyavhengigheter.
Respons	Respons på både planlagte og uplanlagte avslutninger (stressede/ikke-stressede avslutninger).
Operasjonell motstandskraft	Identifikasjon av avhengigheter og koblinger med kontinuitetsplaner og hendelses- og krisekommunikasjon.

*Kravene til en exitplan følger av RTS Third-Party ICT Service Policy, artikkel 10. RTSen krever at det etableres en exitplan for hver kontraktsmessig ordning som underbygger en kritisk eller viktig funksjon. Det blir presisert at i tilfeller hvor exitplaner skal omhandle bytte av IKT-leverandør, så kan exitplanen skrives sammen og ikke for hver enkelt kontrakt med leverandøren.

8.9. Sjekkliste exitplan (4.5.1)

Denne sjekklisten er utarbeidet som et supplement til bruk under utarbeidelse av egne exitplaner. Listen er ikke uttømmende og gir ikke svar på hva som skal gjøres hvis svaret på et spørsmål er nei. Formålet med sjekklisten er for å sikre at de viktigste momentene i DORA er vurdert. Hvis svaret på noen av spørsmålene er nei, bør dette enten gjennomgås som et separat punkt eller kommenteres på hvorfor det ikke har blitt vurdert som et tillegg til planene.

Tematikk	Kontrollspørsmål
Alternative Løsninger	
Identifiser alternative IKT-leverandører	Er det identifisert alternative IKT-leverandører?
Internoverføring	Er det mulighet for å flytte tjenesten in-house?
	Er det gjort vurdering av modenhet for å kunne flytte tjenesten internt?
Avvikling av tjeneste	Må tjenesten avvikles grunnet manglende alternative løsninger?
	Har man adressert risikoen på andre måter?
Leverandørovergang	
Tjenestefortsettelse under exit	Er det etablert en plan for å sikre at tjenesten opprettholdes under overgangen/migrering? DORA 30.3 (f)
Kunnskapsoverføring / kompetanseoverføring	Er det etablert en plan / avtaler for kunnskapsoverføring fra IKT-leverandør?
Tredjeparts kontrakter	Er det vurdert om kontrakter med tredjeparter (underleverandører til IKT-leverandøren) skal være del av en exit plan? Skal eget foretak kunne ta disse kontraktene over eller flyttes til et nytt foretak?
Risikohåndtering	

Migrering	Er det adressert risikoer knyttet til terminering / migrering?
	Hvordan er identifiserte høy risiko aktiviteter eller andre risiko-momenter adressert?
Kundepåvirkning	Er det adressert risikoer knyttet til kundepåvirkning?
	Er kunderelatert påvirkning adressert og planlagt for?
Regulatorisk	Er det adressert risiko for å ikke kunne oppfylle regulatoriske krav?
	Hvordan skal regulatoriske forpliktelser sikres i perioden. Herunder til AML og andre dokumentasjonskrav.
Kontroller	Hvilke ekstra kontroller og prosesser er det nødvendig å implementere i perioden?
Roller	Er det etablert tydelige roller og ansvar i eget selskap ved iverksettelse av Exit plan?
Kompetanse	Hvordan er kompetansen internt for å ta over, eller flytte til annen IKT-leverandør?
Sikring av kundepåvirkning	
Forstyrrelsesfri exit	Er det sikret at en exit ikke nevneverdig påvirker kunde opplevelsen?
Tjenestekvalitet	Er det planlagt for påvirkning på og minimering av reduksjon av kontinuitet av tjenesten og kvalitet til kunder?
Kommunikasjonsplan	Er det utarbeidet en kommunikasjonsplan til kunder som kan bli påvirket av migrering eller exit fra IKT-leverandøren?
Data- og Tilgangshåndtering	

Datahåndtering	Er det planlagt for utlevering, destruksjon eller overføring av data?
	Har det blitt utarbeidet hvilken data som det er behov for? (Feil logger, kundedata, tilgangslogger, dokumentasjon m.m.)
Fjerning av Tilgang	Er det etablert en plan for fjerning av tilgang?
	Hvordan skal dette gjennomføres?
	Skal det etableres ekstra logging i perioden?
Intellektuell eiendom (IP)	Er det etablert en plan / avtale for hva som skjer med utviklet kode og annen IP?
Økonomiske Vurderinger	
Kostnadsvurdering	Er kostnader relatert til alternativer under “alternative løsninger” vurdert?
Migreringskostnader	Er kostnader relatert til migrering evaluert?
Avslutningskostnad	Har det blitt avtalt et vederlag for tidlig avslutning av avtale? Er det forskjeller avhengig av hvorfor den avsluttes tidlig?
Testing og Gjennomgang av Plan	
Testprosedyrer	Er det etablert en plan for hvordan planen kan testes? (Desktop, table-top, annen måte)
	Har man vurdert gjennomførbarhet av testingen? Kan man reelt få testet exit-planen, eller er det kun en compliance aktivitet?
	Har man tilrettelagt for revisjonshistorikk og mulighet for endringer basert på test resultater?

Leverandørinvolvering	Har man vurdert til hvilken grad IKT-leverandøren må være involvert i testing av planen?
	Har man vurdert hvilke deler av exitplanen som skal og kan deles med IKT-leverandør? RTS on Third-Party ICT Service Policy, side 56, presiserer at forretningssensitiv informasjon ikke trenger å bli delt med IKT-leverandør.
Proporsjonalitet og Scenarier	
Scenarier	Er det etablert scenarier som vil trigge en exit?
	Er scenarier, triggerpunkter og krav som kan utløse en exit forankret med IKT-leverandør?
Påvirkning	Er påvirkning på andre exit-planer og IKT-leverandører vurdert?
	Er påvirkning på andre tjenester, som avhenger av denne tjenesten, vurdert?
Intra-gruppe / allianse	
Intra-gruppe / allianse	Er det vurdert hvordan en exit fra avtalen/leverandørforholdet kan påvirke tjenestene innen intra-gruppen/alliansen?
	Er det avklart hvordan en exit fra intra-gruppen/allianseavtalen vil påvirke de gjenværende tjenestene?
	Hvordan vil en exit fra en IKT-leverandør i et intra-gruppeforhold/allianseforhold kunne påvirke andre avtaler som er inngått direkte med leverandøren?

8.10. Triggere exitplan (4.5.1)

Eksempel på triggere for exitplan

#	Eksempler	Krav i DORA
1	**Vedvarende tjenesteavbrudd:** Flere eller langvarige avbrudd i tjenesteleveransen som påvirker kritiske funksjoner.	28.7 c RTS* art. 10
2	**Mislykket tjenesteleveranse:** Gjentatte tilfeller av at IKT-leverandøren ikke oppfyller avtalte servicenivåer, inkludert vedvarende reduksjon av tjenestekvalitet.	28.7 c RTS* art. 10
3	**Uventet kontraktsopphør:** Plutselig oppsigelse av kontrakten fra IKT-leverandørens side.	28.7 a RTS* art. 10
4	**Regulatoriske brudd**: Situasjoner der IKT-leverandøren ikke lenger oppfyller regulatoriske krav, inkludert nye krav.	28.7 a
5	**Sikkerhetsbrudd:** Alvorlige sikkerhetsbrudd som setter sensitive data eller systemer i fare.	28.7 c
6	**Finansiell instabilitet hos IKT-leverandør:** Tegn på økonomiske vanskeligheter som kan påvirke leveransen	28.7 a
7	**Endringer i forretningsstrategi:** Endringer som gjør tjenestene unødvendige.	-
8	**Endringer i eierstruktur:** Oppkjøp eller fusjoner som påvirker IKT-leverandørens evne til å levere tjenester.	28.7 a
9	**Nøkkelpersoner:** Tap av sentrale nøkkelpersoner som kan forringe kvaliteten.	28.7 b
10	**Underleverandører:** Uønsket bruk av underleverandører, eller konflikt mellom IKT-leverandøren og underleverandører som kan påvirke tjenesten.	28.7 b
11	**Tilsynsproblemer:** Situasjoner der tilsyn fra myndighetene blir hindret.	28.7 d
12	**Svak governance:** Situasjoner hvor IKT-leverandøren viser vedvarende svak styring og kontroll.	28.7 c

* RTS on Third-Party ICT Service Policy

8.11. Revisjon av exitplan (4.5.1)

Eksempel på hendelser hvor revisjon av exitplan er nødvendig

#	Eksempler
1	**Endringer i leverandørforholdet:** Nye kontraktsvilkår eller endringer i IKT-leverandørens status.
2	**Nye regulatoriske bestemmelser:** Oppdateringer i lovgivning som påvirker tjenesteleveransen.
3	**Endret kritikalitet i BIA:** Business Impact Analysis (BIA) har endret vurderingen av tjenestens kritikalitet / viktighet.
4	**Endringer i tjenestens natur:** Tjenesten har utviklet seg eller endret seg betydelig. Dette gjelder også hvis den forretningsmessige prosessen har endret seg, men leverandørforholdet og leveransen er lik.
5	**Flere IKT-leverandører tilgjengelig:** Nye IKT-leverandører har kommet på banen, som kan påvirke valgmulighetene.
6	**Testing avdekker mangler:** Testresultater viser at planen ikke er gjennomførbar eller trenger forbedringer.
7	**Nye avhengigheter:** Nye avhengigheter har oppstått siden forrige gjennomgang.
8	**Nøkkelpersoner:** Endring i nøkkelpersoner som støtter tjenesten hos IKT-leverandøren eller i eget foretak.
9	**Kontinuitetsplaner:** Det har vært gjort endringer i kontinuitetsplanene som støtter tjenesten.