Næringslivets sikkerhets-råd

Styring av IKT-leverandørrisiko i matbransjen

bama

TINE

Felleskjøpet

NorgesGruppen

Nortura
bondens selskap

coop

Orkla Foods

REMA 1000

Tittel	Styring av IKT-leverandørrisiko i matbransjen
Forfatter	Bjarte Malmedal
Utgave og år	Første utgave, 2025
Sponsorer	Utgitt med faglig bidrag fra Tine, Orkla Foods, Felleskjøpet Agri, Coop, Norgesgruppen, Rema 1000, Nortura og Bama
Opphavsrett	Opphavsrett (c) 2025 Næringslivets sikkerhetsråd
Medvirkende	Omslagsdesign og innvendig design: Christian von Schack
Bilder	**Forsideillustrasjon**: Generert med Google Gemini. **Foto** s.11: ASKO; foto s.12 og s.44: TINE; foto s.21: Anders Rikstad; foto s.23, s.25, s.33, s.53, s.59 og s.74-75: BAMA; foto s.26: John Trygve Tollefsen; foto s.55: Jostein Vedvik; foto s.62: MATBØRSEN; foto s.65: Jostein Vedvik.
ISBN	ISBN 978-82-694361-0-5
Kopierings-informasjon	Det må ikke kopieres fra veilederen i strid med åndsverksloven. Ta kontakt med Næringslivets sikkerhetsråd dersom du ønsker å kopiere eller bruke deler av veilederen.

Sponsorer

NHO Service og Handel

VIRKE

NHO Mat og Drikke

INNHOLD

Forord	
1. Formål med veilederen	5
2. Veilederens oppbygging	7
3. Leverandørrisikostyring under NIS2	9
3.1 Vesentlige vs. viktige virksomheter	10
3.1.1 IKT-tjenester i matbransjen er mer enn bare IT	10
4. Helhetlig styring av IKT-leverandørrisiko	13
4.1. Planlegging	14
4.1.1. Behovsanalyse og kravspesifikasjon	14
4.1.2. Innledende kritikalitetsvurdering	15
4.1.3. Markedsanalyse og strategiske hensyn	15
4.2. Vurdering og valg av IKT-leverandør	16
4.2.1. Vurdering av kritikaliteten på leveransen til IKT-leverandøren	16
4.2.2. Risikovurdering av IKT-leverandører	17
4.2.3. Hensynet til konkurranseloven	17
4.3. Avtaleinngåelse og oppstartsfase	19
4.3.1. Standardiserte maler for kontrakter og vedlegg	19
4.3.2. Sjekkliste for IKT-leverandøravtaler	19
4.4. Kontinuerlig oppfølging og overvåking	20
4.4.1. Sjekkliste for oppfølging av IKT-leverandører	20
4.4.2. Oppfølgning av uavhengige vurderinger	20
4.4.3. Håndtering og rapportering av hendelser	20
4.5. Exitstrategi og avslutning av samarbeid	22
5. Ordliste	23
6. Referanser	25
7. Vedlegg	27
Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen	28
Vedlegg B: Standard sjekkliste for risikovurdering av leverandører	34
Vedlegg C: Standardiserte krav til kontrakter og vedlegg	40
Vedlegg D: Sjekkliste for oppfølging av IKT-leverandører	46
Vedlegg E: Innhold til exitplan	54
Vedlegg F: Sjekkliste for exitplan	66
Vedlegg G: Triggere for iverksettelse av exitplan	70

FORORD

I et stadig mer digitalisert samfunn er matbransjens evne til å håndtere IKT-leverandørrisiko en forutsetning for forsyningssikkerhet og bransjens tillit i samfunnet. Matindustrien er en samfunnskritisk funksjon, og dens robusthet hviler nå like mye på digitale systemer som på fysisk infrastruktur. Den kommende innføringen av EU-direktivet om nettverks- og informasjonssikkerhet (NIS2) krever at bransjen har en omfattende og integrert forståelse av digital og fysisk motstandskraft.

NIS2-direktivet stiller krav til en strukturert og helhetlig tilnærming til IKT-leverandørrisiko. Nasjonal sikkerhetsmyndighet (NSM) understreker i sine trusselvurderinger et skjerpet risikobilde[1], der sabotasje og angrep mot leverandørkjeder er sannsynlige scenarioer. Matproduksjon, -foredling og -distribusjon er eksplisitt utpekt som en sektor som omfattes av det nye regelverket, noe som utvider antallet regulerte virksomheter[2] i Norge.

For at tiltakene skal være effektive, må de være sammenlignbare og gjenkjennelige på tvers av aktører i næringen og i hele leverandørkjeden, fra råvareprodusenter og utstyrsleverandører til logistikkpartnere og dagligvarehandel. Denne veilederen har som mål å være et praktisk verktøy for virksomheter i matbransjen som ønsker å styrke sin styring av IKT-leverandørrisiko. Den skal bidra til å standardisere praksis og styrke samarbeidet i en sektor hvor avhengighetene er mange og komplekse.

Denne veilederen er utarbeidet i samarbeid med bransjeaktørene som inngår i prosjektet CYMAT. Vi retter en stor takk til alle som har bidratt med sin tid og innsikt.

Odin Johannessen

Direktør NSR

1 Risiko 2025 - Nasjonal sikkerhetsmyndighet, brukt juni 23, 2025, https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2025

2 NIS2: Hvilke virksomheter og leveranser vil omfattes av fremtidens krav til cybersikkerhet infrastruktur? | Lov&Data, brukt juni 23, 2025, https://lod.lovdata.no/article/2025/03/NIS2%20Hvilke%20virksomheter%20og%20leveranser%20vil%20omfattes%20av%20fremtidens%20krav%20til%20cybersikkerhet%20infrastruktur

1.

Formål med veilederen

Formålet med denne veilederen er å hjelpe virksomheter i matbransjen med å styre leverandørrisiko knyttet til informasjons- og kommunikasjonsteknologi (IKT) på en systematisk og effektiv måte og i tråd med kravene i EUs NIS2-direktiv (heretter NIS2). IKT-leverandører, både for administrative systemer (IT) og produksjons-systemer (operasjonell teknologi, OT), spiller en kritisk rolle i matsektoren. Mangelfull styring kan medføre betydelige risikoer knyttet til produksjonsstans, matsikkerhet, kvalitet og etterlevelse av regelverk.

Matbransjen er definert som viktige virksomheter[3] under NIS2. Dette innebærer et særlig ansvar for å beskytte operasjonell stabilitet og sikre kontinuitet i matforsyningen. Ettersom mange virksomheter er avhengige av en kompleks kjede av leverandører for kjernefunksjoner som råvarer, produksjonsutstyr, automasjon, sporingsteknologi, logistikk og databehandling, er en strukturert tilnærming til risikostyring helt avgjørende.[4] En sårbarhet hos én enkelt leverandør kan forplante seg og få alvorlige konsekvenser for hele verdikjeden.[5]

Effektiv styring av leverandørrisiko krever at virksomhetene ikke bare gjennomfører isolerte vurderinger av enkeltleverandører. Den må inkludere en grundig analyse av hvordan ulike aktører, inkludert underleverandører, påvirker hverandre. En slik tilnærming legger grunnlaget for mer presise risikovurderinger og styrker virksomhetens evne til å ivareta operasjonell robusthet.

Denne veilederen skal støtte virksomhetene og leverandørene i matbransjen i deres arbeid med:

Systematisk styring

Hjelpe virksomhetene med å identifisere og vurdere risikoer knyttet til IKT-leverandører, inkludert leverandører av OT-systemer, og å etablere effektive kontrolltiltak for å sikre at leverandører og underleverandører oppfyller nødvendige krav.

Etterlevelse av regelverk

Veilede virksomhetene i å oppfylle regulatoriske krav i NIS2, med særlig fokus på Artikkel 21 om risikostyringstiltak og Artikkel 23 om rapporteringsplikt ved hendelser.

Beskyttelse av kritiske prosesser

Redusere sannsynligheten for at feil eller sikkerhetsbrudd hos IKT-leverandører får alvorlige konsekvenser for produksjonskontinuitet og matsikkerhet.

Ved å bruke denne veilederen får virksomheter og leverandører i matbransjen en felles referanseramme som kan styrke samarbeidet og bedre oppfølging for alle parter. Veilederen bidrar til økt grunnsikring i bransjen, og legger til rette for mer kostnadseffektive løsninger og god konkurranse ved at forventningene er kjent og forutsigbare.

3 ibid

4 OT Networks Are Low-Hanging Fruit for Supply Chain Attacks - SCADAfence Blog, brukt juni 23, 2025, https://blog.scadafence.com/ot-networks-are-the-low-hanging-fruit-for-supply-chain-attacks

5 The digital implications of supply chains - Hinrich Foundation, brukt juni 23, 2025, https://www.hinrichfoundation.com/research/article/digital/the-digital-implications-of-supply-chains/

2.

Veilederens oppbygging

Denne veilederen gir en overordnet innføring i styring av leverandør-risiko med et særlig fokus på digital sikkerhet. Veilederen er utformet for å hjelpe aktører i matbransjen med å identifisere, vurdere, overvåke og håndtere risiko knyttet til leverandørforhold.

Den tar utgangspunkt i de fem hovedfasene i livssyklusen til en leverandørrelasjon:

1. **Planlegging.**
   Forberedelse og identifisering av behov og risiko knyttet til tjenesteleveransen.
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 hjelpemidler for løpende overvåking og evaluering av leverandørytelse og risiko.
5. **Exit-strategi og avslutning av samarbeidet.**
   Planlegging og gjennomføring av en strukturert avslutning av leverandørforholdet når det er nødvendig.

Veilederen inkluderer praktiske sjekklister og maler som kan brukes for å styrke risikostyringsprosessene. Virksomhetene må selv vurdere hvilke steg, krav og tiltak som er relevante og nødvendige i den enkelte prosess, og som er anvendelige for den enkelte bedrift.

3.

Leverandør-risikostyring under NIS2

Leverandørrisikostyring er prosessen med å identifisere, vurdere, overvåke og redusere risiko forbundet med bruk av eksterne leverandører. NIS2 formaliserer og stiller krav til slik risikostyring for å sikre et høyt felles cybersikkerhetsnivå i samfunnskritiske sektorer. For matbransjen innebærer dette at ansvaret omfatter den digitale sikkerheten hos et bredt spekter av partnere og leverandører.

Med innføringen av NIS2 utvides virkeområde, og direktivet omfatter et bredt spekter av risiko relatert til alle eksterne IKT-leverandører. Dette inkluderer tradisjonell utkontraktering av IT-tjenester, men også leverandører av operasjonell teknologi (OT) og andre former for tjenestekjøp fra tredjeparter. Tilnærmingen krever en helhetlig forståelse av risiko knyttet til alle eksterne partnere som har tilgang til virksomhetens nettverk og informasjonssystemer.

3.1 Vesentlige vs. viktige virksomheter

NIS2 skiller mellom to kategorier virksomheter, basert på størrelse og kritikalitet. Kategorien avgjør hvilket tilsynsregime virksomheten er underlagt og sanksjonene ved manglende etterlevelse.

Tabell 1 Vesentlige vs. viktige virksomheter

Kategori	Kriterier(Ansatte / Omsetning)	Tilsynsregime	Maksimal sanksjon (det høyeste av)
Vesentlig virksomhet	≥250 ansatte ELLER omsetning >€50 millioner	Proaktivt	€10 millioner ELLER 2% av global omsetning
Viktig virksomhet	≥50 ansatte ELLER omsetning >€10 millioner	Reaktivt	€7 millioner ELLER 1.4% av global omsetning

3.1.1 IKT-tjenester i matbransjen er mer enn bare IT

Et helhetlig fokus på sikkerhet krever at vi også ser helhetlig på IKT-tjenester. Det betyr at vi må se informasjonsteknologi (IT) og operasjonell teknologi (OT) i sammenheng.

NIS2 omtaler ikke OT direkte, men vi bør likevel se OT-sikkerhet som en del av helheten under NIS2-direktivet fordi den tette integrasjonen mellom IT- og OT-systemer betyr at de ikke lenger kan sikres isolert. Et angrep på et kontornettverk (IT) kan spre seg til produksjonssystemer (OT) som styrer fysiske prosesser. Direktivet anerkjenner dette ved å kreve en «tilnærming som dekker alle farer» som beskytter både «nettverks- og informasjonssystemer og det fysiske miljøet til disse systemene». En svikt i OT-sikkerheten kan føre til alvorlige konsekvenser som produksjonsstans, miljøskader eller fare for liv og helse. I denne veilederen definerer vi derfor både IT og OT som en del av IKT-begrepet.

NIS2 Artikkel 21 krever[6] tiltak som beskytter både«nettverks- og informasjonssystemer og det fysiske miljøet til disse systemene». Dermed blir styring av OT-leverandører en kjerneoppgave i leverandørrisikostyringen.

6 NIS 2 Directive, Article 21: Cybersecurity risk-management measures, brukt juni 21, 2025, https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

- **IT** inkluderer systemer for forretningsstøtte, som skytjenester, ERP-systemer (Enterprise Resource Planning), leverandørportaler, logistikksystemer og administrative verktøy.
- **OT** er systemene som direkte overvåker og styrer industrielle prosesser. I matbransjen er dette kritisk infrastruktur som inkluderer:

    - Systemer for prosesskontroll (f.eks. SCADA) som styrer produksjonslinjer
    - Systemer for overvåking av kjølekjeden (cold chain monitoring)
    - Digitale sporbarhetssystemer (traceability)
    - Produksjonsstyringssystemer (Manufacturing Execution Systems)
    - Tjenester fra leverandører som utfører vedlikehold og oppgraderinger på dette utstyret, ofte via fjerntilgang.[7]

For matbransjen innebærer dette at leverandører av produksjonsutstyr og -programvare (OT) må behandles som potensielt kritiske IKT-leverandører. Den økende digitaliseringen og sammensmeltingen av IT og OT bidrar til å skape en betydelig større angrepsflate.[8] En vedlikeholdstekniker fra en leverandør som kobler en laptop til produksjonsnettverket, eller en kompromittert programvareoppdatering til et SCADA-system, kan representere en direkte vei til å manipulere, sabotere eller stanse den fysiske produksjonen. Dette er en risiko med direkte fysiske konsekvenser, som kan true både matsikkerhet og forsyningssikkerhet.

7 SCADA Risk Management: Protecting Critical Infrastructure - Claroty, brukt juni 23, 2025, https://claroty.com/blog/scada-risk-management-protecting-critical-infrastructure

8 Revisiting Threats to Food & Beverage Cybersecurity | TXOne Networks, brukt juni 23, 2025, https://www.txone.com/blog/revisiting-threats-to-food-beverage-cybersecurity/


0292
0292

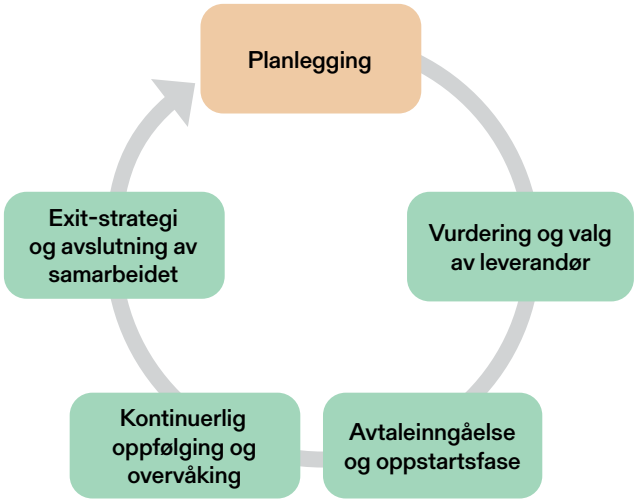
4.

Helhetlig styring av IKT-leverandørrisiko

En helhetlig tilnærming til styring av IKT-leverandørrisiko innebærer å etablere en oversikt over alle IKT-leverandører og deres underleverandører, og å gjennomføre systematiske konsekvensanalyser (Business Impact Analysis, BIA) for å identifisere hvilke leverandører og funksjoner som er kritiske for virksomheten. Dette danner grunnlaget for å utvikle krav, velge leverandører, følge dem opp og planlegge for en kontrollert avslutning av samarbeidet.

4.1. Planlegging

For å sikre et godt utgangspunkt for et vellykket samarbeid, er det viktig å starte med grundige forberedelser i tidlige faser. En strukturert planlegging er god forretningspraksis og en forutsetning for å møte de skjerpede kravene i NIS2-direktivet. Dette innebærer blant annet:



4.1.1. Behovsanalyse og kravspesifikasjon

Før man går ut i markedet, må virksomheten ha en klar forståelse av hva den trenger, med tanke på funksjonelle krav og krav til sikkerhet.

- **Identifiser behovene**
  Kartlegg hvilke tjenester eller produkter som er nødvendige for å støtte forretningsprosessene. Det er spesielt viktig å vurdere hvordan en ny tjeneste vil integreres med og påvirke både eksisterende produksjonssystemer (OT) og forretningssystemer (IT).
- **Definer sikkerhetskravene**
  Sikkerhet må være en integrert del av kravspesifikasjonen fra start.
- **Krav til forretningskontinuitet**
  Basert på virksomhetens egen konsekvensanalyse (BIA), definer krav til oppetid, gjenopprettingstid (RTO) og maksimalt akseptabel nedetid (MTPD). Disse kravene vil være styrende for servicenivå-avtalene (SLA) i kontraktsfasen.

4.1.2. Innledende kritikalitetsvurdering

Før man vurderer spesifikke leverandører, må virksomheten vurdere kritikaliteten til selve tjenesten som skal anskaffes. Denne tidlige vurderingen, basert på prinsippene i Vedlegg A, avgjør hvor dyptgående de videre prosessene må være.

- **Vurder konsekvens**
  Hva er konsekvensene dersom denne tjenesten svikter? Vurder innvirkning på forsyningssikkerhet, matsikkerhet, regulatorisk etterlevelse, økonomi og omdømme.
- **Vurder avhengighet**
  Hvor avhengig vil virksomheten bli av denne tjenesten? Er den basert på standardisert eller proprietær teknologi? Hvor lett vil det være å bytte til en alternativ løsning senere?

Resultatet av denne innledende vurderingen gir en pekepinn på om leveransen sannsynligvis vil falle i kategorien «høy», «medium» eller «lav prioritet», noe som styrer grundigheten i de neste fasene.

4.1.3. Markedsanalyse og strategiske hensyn

Med en klar kravspesifikasjon og en forståelse av tjenestens kritikalitet, kan virksomheten undersøke markedet.

- **Kartlegging av leverandører**
  Identifiser tilgjengelige IKT-leverandører som kan møte kravene. Vurder deres kapasitet, historikk, omdømme og spesifikke erfaring fra matbransjen, inkludert dokumentert kompetanse på OT-sikkerhet.
- **Vurdering av konsentrasjonsrisiko**
  Undersøk om markedet er dominert av få aktører. En høy avhengighet til én enkelt leverandør for flere kritiske funksjoner, eller at hele bransjen bruker samme leverandør, utgjør en systemisk risiko som bør vurderes tidlig.
- **Hensyn til konkurranse**
  Utform kravene slik at de er proporsjonale med risikoen og så langt som mulig teknologinøytrale. Dette for å unngå unødvendige barrierer for mindre eller nye leverandører som kan tilby innovative løsninger, i tråd med konkurranselovgivningen.
- **Planlegging for hele livssyklusen**
  Tenk på avslutning av samarbeidet allerede i planleggingsfasen. Vurderingen av avhengighet (punkt 2) er direkte relevant for en fremtidig exitstrategi. En leverandør som benytter proprietær teknologi som er vanskelig å migrere fra, vil kreve en langt mer detaljert exitplan.

Resultatet av planleggingsfasen skal være et solid beslutningsgrunnlag for den videre prosessen. Dette inkluderer en detaljert kravspesifikasjon, en innledende kritikalitetsvurdering, en oversikt over aktuelle leverandører i markedet, og en forståelse for de langsiktige strategiske implikasjonene av anskaffelsen.

4.2. Vurdering og valg av IKT-leverandør

Due diligence er en sentral del av styring av leverandørrisiko 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, fordi feil hos disse kan få betydelige konsekvenser for virksomhetens drift.

4.2.1. Vurdering av kritikaliteten på leveransen til IKT-leverandøren

Når virksomheten har gjennomført en konsekvensanalyse (BIA) av sine forretningsprosesser og tjenester, vil denne analysen danne grunnlaget for å vurdere kritikaliteten til leverandørens tjeneste.

- **Kritikalitet**
  Vurderes ut fra BIA. En prosess eller tjeneste er kritisk hvis et avbrudd truer:

  1. **Forsyningssikkerhet**, altså evnen til å levere mat til samfunnet.
  2. **Matsikkerhet**, altså risiko for forurensning, feil ingrediensblanding, brudd i kjølekjeden eller andre forhold som gjør maten utrygg.
  3. **Regulatorisk etterlevelse**, eller evnen til å overholde lovpålagte krav til sporing og dokumentasjon.

- **Avhengighet**
  Vurderes ut fra hvor lett leverandøren kan erstattes. En leverandør av en standardisert skytjeneste kan ha lav avhengighet. En leverandør av en proprietær SCADA-plattform som styrer en hel fabrikk, eller en spesialisert leverandør av sporingsløsninger for en kompleks forsyningskjede, vil representere en svært høy avhengighet.

Basert på en vekting av disse to faktorene kan leveransen kategoriseres som ikke-kritisk, betydningsfull eller kritisk/viktig, noe som styrer nivået på videre oppfølging.

Se Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen

4.2.2. Risikovurdering av IKT-leverandører

Som en del av due diligence-prosessen må virksomheten gjennomføre en risikovurdering for å identifisere potensielle utfordringer. Denne vurderingen må dekke de ti minimumstiltakene i NIS2 Artikkel 21 og spesifikt vurdere leverandørens evne til å sikre sin del av leverandørkjeden. Virksomheten kan vurdere om sertifiseringer og tredjepartsrevisjoner er tilstrekkelig som grunnlag for å vurdere risiko knyttet til IKT-leverandøren, som et alternativ til å gjennomføre slike vurderinger på selvstendig grunnlag.

Denne veilederen presenterer ikke et fullstendig rammeverk for risikovurdering, og det forutsettes at den enkelte virksomhet har et slikt rammeverk. Vedlegg B: Standard sjekkliste for risikovurdering av IKT-leverandører inneholder vurderingspunkter som vil være til nytte for virksomheter og leverandører i matbransjen. Sjekklisten er ment som et supplement til virksomhetens rammeverk for risikovurdering og -styring.

4.2.3. Hensynet til konkurranseloven

Denne veilederen er utformet for å styrke sikkerheten og robustheten i matbransjen. En robust digital infrastruktur og en sikker leverandørkjede er nødvendig for å beskytte både produksjon, distribusjon og forbrukertillit. Samtidig er det viktig å anerkjenne konkurranserettslige forhold når det utvikles veiledere for hele bransjen.

Ved implementering av veilederens anbefalinger, skal virksomhetene aktivt vurdere hvordan dette påvirker konkurransen i markedet. Målet er å sørge for at en holder seg innenfor konkurranseloven og å unngå unødvendige barrierer for nye eller mindre leverandører som kan tilby innovative og kostnadseffektive løsninger. Samtidig er det nødvendig å forholde seg til de kravene som stilles til styring av IKT-leverandørrisiko i lov og forskrift.

Dette er spesielt relevant i et marked der etablerte aktører ofte har betydelige ressurser til å oppfylle omfattende krav, mens mindre selskaper kan slite med å komme inn på tross av at disse kan være nyskapende.

For å forebygge konkurransevridning oppfordres virksomhetene til å vurdere følgende:

a. Praktiser proporsjonalitet

Tilpass kravene til sikkerhet og dokumentasjon basert på leveransens faktiske kritikalitet og risiko, slik det er beskrevet i Vedlegg A og B. Dette innebærer at en leverandør av et kritisk SCADA-system for produksjonslinjen naturligvis vil underlegges strengere krav enn en leverandør av standard kontorprogramvare. Unngå å stille unødig strenge krav til ikke-kritiske leveranser, fordi dette kan ekskludere

mindre leverandører uten at det gir en reell sikkerhetsgevinst. En grundig risikovurdering bør alltid ligge til grunn for hvilke krav som stilles, slik at ressursene rettes mot de områdene med størst potensiell konsekvens.

b. Teknologinøytralitet
Der det er mulig, fokuser på sikkerhetsmål og -funksjonalitet fremfor spesifikke teknologier eller sertifiseringer. Dette betyr at i stedet for å kreve en spesifikk ISO 27001-sertifisering, kan man be om dokumentasjon som viser at leverandøren har et styringssystem for informasjonssikkerhet som oppnår tilsvarende sikkerhetsnivå. Dette åpner for at leverandører kan oppfylle kravene på ulike måter, basert på deres egne løsninger, metoder og innovative tilnærminger, uten å være bundet til en bestemt standard eller plattform.

c. Alternative bevis
Aksepter ulike former for dokumentasjon og bevis på sikkerhetstiltak, dersom disse viser at tilsvarende sikkerhetsnivå oppnås. Dette kan inkludere interne revisjonsrapporter, kundereferanser fra andre anerkjente virksomheter, eller andre relevante attester som bekrefter leverandørens sikkerhetspraksis. Det kan også inkludere automatiserte løsninger som kan effektivisere rapportering og dokumentasjon.

Dette er spesielt viktig for mindre leverandører eller oppstartsbedrifter som kanskje ikke har råd til de kostbare og tidkrevende sertifiseringene som større selskaper ofte besitter. Fleksibilitet i dokumentasjonskrav kan bidra til å senke inngangsbarrierene og fremme et mer mangfoldig leverandørmarked.

d. Dialog og samarbeid
Opprettholde en åpen dialog med potensielle leverandører om sikkerhetskrav og forventninger, og vær villig til å diskutere tilpasninger der det er hensiktsmessig og ikke kompromitterer sikkerheten. En proaktiv tilnærming der virksomhetene veileder og samarbeider med leverandører om hvordan kravene kan oppfylles, kan bidra til å bygge kompetanse i markedet og sikre at flere aktører kan konkurrere. Dette kan også bidra til å identifisere innovative løsninger som kanskje ikke var åpenbare ved en rigid tolkning av kravene.

e. Overvåk markedet
Kontinuerlig følg med på utviklingen i leverandørmarkedet for IKT-tjenester, for å sikre at det er tilstrekkelig konkurranse og at nye aktører får mulighet til å etablere seg. Dette innebærer å vurdere om kravene i veilederen utilsiktet fører til en konsentrasjon av leverandører, og eventuelt juster praksis for å motvirke dette. En jevnlig markedsanalyse kan avdekke om det er tilstrekkelig tilbud av kvalifiserte leverandører, og om det er rom for nye aktører til å vokse og tilby sine tjenester.

4.3. Avtaleinngåelse og oppstartsfase

Avtaleinngåelses- og oppstartsfasen er en kritisk del av leverandørrisikostyringen, hvor virksomheten formaliserer samarbeidet med IKT-leverandøren.

4.3.1. Standardiserte maler for kontrakter og vedlegg

Kontrakter med IKT-leverandører er både kommersielle avtaler og sentrale styringsdokumenter for sikkerhet. Avtalene må gi virksomheten rett til å vurdere og revidere leverandørens sikkerhetspraksis og kreve forbedringer ved avvik.[9] Kontrakten skal spesifisere krav til blant annet:

- IKT-sikkerhet, personvern og tilgangskontroll
- Sårbarhetshåndtering og sikker utvikling av programvare
- Bruk av kryptering
- Leverandørens plikt til å informere om og stille krav til sine underleverandører
- Prosedyrer for hendelseshåndtering og varsling som er i tråd med virksomhetens egen rapporteringsplikt.

4.3.2. Sjekkliste for IKT-leverandøravtaler

Bedriften bør bruke en praktisk sjekkliste for å sikre at alle relevante krav fra NIS2, spesielt Artikkel 21(2)(d)[10] om leverandørkjedesikkerhet, er oversatt til konkrete og etterprøvbare avtalepunkter. Sjekklisten bør dekke rettigheter og forpliktelser, servicenivåer (SLA), krav til bistand ved hendelser, og vilkår for avslutning av avtalen.

Se Vedlegg C: Standardiserte krav til kontrakter og vedlegg.

9 Blogg: NIS2 endrer spillereglene for leverandørstyring - BDO, brukt juni 25, 2025, https://www.bdo.no/nb-no/bloggen/nis2-endrer-spillereglene-for-leverandorstyring

10 NIS 2 Directive, Article 21: Cybersecurity risk-management measures, brukt juni 21, 2025, https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

4.4. Kontinuerlig oppfølging og overvåking

Denne fasen handler om å sikre at avtalt sikkerhetsnivå opprettholdes over tid gjennom dynamisk og risikobasert oppfølging.

4.4.1. Sjekkliste for oppfølging av IKT-leverandører

Oppfølgingen kan struktureres i tre nivåer: strategisk (ledelsesnivå), taktisk (avtalestyring) og operasjonell (daglig leveranse). Dette inkluderer jevnlige møter, gjennomgang av ytelsesrapporter og vurdering av uavhengige tredjepartsattestasjoner, som for eksempel en ISO 27001-sertifisering.

Se Vedlegg D: Sjekkliste for oppfølging av IKT-leverandører.

4.4.2. Oppfølgning av uavhengige vurderinger

For kritiske og viktige leverandører bør innhenting og vurdering av uavhengige bekreftelser av internkontrollen være en del av den årlige oppfølgingen. Slike rapporter (f.eks. ISAE 3402, SOC 2) gir en uavhengig vurdering av hvorvidt leverandørens systemer og kontroller oppfyller spesifikke sikkerhetsstandarder. Eventuelle avvik i rapportene må følges opp med leverandøren for å sikre at tilstrekkelige korrigerende tiltak iverksettes.

4.4.3. Håndtering og rapportering av hendelser

Den strenge og trinnvise rapporteringsplikten i NIS2 Artikkel 23[11] gjør at hendelseshåndtering ikke er en isolert og intern prosess. Det er en felles forpliktelse som krever integrasjon med leverandørenes prosesser for hendelseshåndtering. En forsinkelse hos en leverandør kan direkte føre til at virksomheten selv bryter loven.

11 NIS 2 Directive, Article 23: Reporting obligations, brukt juni 21, 2025, https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html

Prosessen starter med at en hendelse oppstår hos en leverandør, for eksempel en skytjeneste-leverandør eller en OT-leverandør. Virksomheten blir først klar over hendelsen når den blir informert av leverandøren. NIS2 Artikkel 23 krever et tidlig varsel til nasjonale myndigheter (I Norge er dette NSM/NCSC) innen 24 timer etter at man er blitt klar over en betydelig hendelse. Dette betyr at leverandørens kontraktsfestede varslingsfrist (SLA) må være tilstrekkelig kort til at virksomheten kan overholde sin egen 24-timersfrist.

Videre krever NIS2 et mer detaljert hendelsesvarsel innen 72 timer, som skal inneholde en «innledende vurdering, inkludert alvorlighetsgrad og innvirkning». Å produsere denne vurderingen er svært krevende uten teknisk informasjon og samarbeid fra leverandøren.

Konsekvensen av dette er at hendelseshåndtering må være en tett koordinert, kontraktfestet og jevnlig øvet prosess mellom virksomheten og dens kritiske leverandører.

Tabell 2 Rapporteringskrav jf. Artikkel 23

Tidsfrist	Rapporttype	Minimumskrav til innhold	Ansvarlig
Innen 24 timer	Tidlig varsel	Indikasjon eller mistanke om at en sikkerhetshendelse har funnet sted og konsekvensvurdering av denne.	Virksomheten (til NCSC)
Innen 72 timer	Hendelsesvarsel	Oppdatert informasjon, innledende vurdering av alvorlighets-grad/innvirkning, indikatorer på kompromittering (IoCs).	Virksomheten (til NCSC)
Etter forespørsel	Mellomrapport	Statusoppdateringer	Virksomheten (til NCSC)
Innen 1 måned	Sluttrapport	Detaljert beskrivelse, rotårsak, iverksatte tiltak og endelig konsekvensvurdering.	Virksomheten (til NCSC)

Dersom hendelsen også involverer risiko for personopplysninger, vil GDPR-regelverket stille krav om rapportering til Datatilsynet. Dette perspektivet dekkes ikke av denne veilederen.

4.5. Exitstrategi og avslutning av samarbeid

Utarbeidelse av exitstrategier for kritiske og viktige IKT-leverandører er en viktig del av leverandør-risikostyringen. En god exitstrategi sikrer en kontrollert og strukturert avslutning av samarbeidet, enten det er planlagt eller skjer som følge av en krise.

I matbransjen må exitplaner spesielt ta høyde for utfordringene med å overføre data, systemer og kompetanse knyttet til komplekse og ofte proprietære OT-systemer. Å bytte leverandør for et SCADA-system som styrer en hel fabrikk er en betydelig operasjon som krever lang planlegging. Muligheten for å ta driften internt («in-housing») kan være begrenset på kort sikt. Derfor må exitplanen være en integrert del av virksomhetens overordnede planer for forretningskontinuitet og katastrofegjenoppretting, slik det kreves i NIS2 Artikkel 21(2)(c)[12].

Planen må dekke:

- Overføring eller sikker sletting av data.
- Overføring av kunnskap og kompetanse.
- Vurdering av alternative leverandører eller interne løsninger.
- En realistisk tidslinje som sikrer kontinuitet i kritiske funksjoner som produksjon, kjølekjedekontroll og sporing under overgangen.

Se vedleggene:

- Vedlegg E: Innhold til exitplan for kritiske og viktige IKT-leverandører
- Vedlegg F: Sjekkliste for exitplan
- Vedlegg G: Triggere for iverksettelse av exitplan

12 NIS 2 Directive, Article 21: Cybersecurity risk-management measures, brukt juni 21, 2025, https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

5. Ordliste

BIA (Business Impact Analysis): Konsekvensanalyse. En prosess for å identifisere og evaluere de potensielle effektene av en driftsstans på kritiske forretningsprosesser.

CSIRT (Computer Security Incident Response Team): En gruppe eksperter som håndterer sikkerhetshendelser. Hver medlemsstat under NIS2 skal ha nasjonale CSIRT-er. I Norge er dette NSM/NCSC.

Cyberhygiene: Grunnleggende sikkerhetspraksis som alle ansatte bør følge, som bruk av sterke passord, oppdatering av programvare og å være på vakt mot phishing.

CYMAT: Et prosjekt i matbransjen som har som mål å styrke den enkelte bedrifts cybersikkerhet og ivareta bransjens fellesinteresser innen cybersikkerhet.

Due diligence: En grundig undersøkelsesprosess av en leverandør før en avtale inngås, for å kartlegge risiko innen områder som økonomi, sikkerhet og omdømme.

ERP (Enterprise Resource Planning): Forretningsstyringssystem. Store, integrerte programvaresystemer som håndterer en virksomhets kjerneområder som økonomi, logistikk, produksjon og personal.

IKT-tjenester: Digitale og datadrevne tjenester. Under NIS2 omfatter dette både IT-systemer (administrative) og OT-systemer (produksjonsstyring).

IT (Informasjonsteknologi): Teknologi der informasjon bearbeides, lagres og formidles som tekst, lyd eller bilder i digital form.

Leverandørkjedesikkerhet: Tiltak for å håndtere og redusere risiko som oppstår fra leverandører og deres underleverandører i en forsyningskjede.

MES: Manufacturing Execution System - Produksjonsstyringssystem.

NIS2: EU-direktiv (2022/2555) om tiltak for et høyt felles cybersikkerhetsnivå i hele Unionen. Implementeres i Norge gjennom digitalsikkerhetsloven.

NSM (Nasjonal sikkerhetsmyndighet): Norges direktorat for forebyggende nasjonal sikkerhet, som har en sentral rolle i oppfølgingen av NIS2.

OT (Operasjonell teknologi): Maskinvare og programvare som oppdager eller forårsaker en endring gjennom direkte overvåking og/eller kontroll av fysiske enheter, prosesser og hendelser i virksomheten.

Proporsjonalitet: Et prinsipp om at tiltak (f.eks. sikkerhetskrav) skal stå i rimelig forhold til den risikoen de skal redusere. Man stiller strengere krav til en kritisk leverandør enn til en ikke-kritisk leverandør.

RTO (Recovery Time Objective): Gjenopprettingstid. Det tidsrommet en forretningsprosess maksimalt kan være nede etter en hendelse før konsekvensene blir uakseptable.

SCADA (Supervisory Control and Data Acquisition): Et system for fjernovervåking og -styring av industrielle prosesser.

SLA (Service Level Agreement): Tjenestenivåavtale. En del av en kontrakt som definerer det avtalte nivået på en tjeneste, for eksempel krav til oppetid, responstid ved feil og varslingstid ved hendelser.

Sporbarhet (Traceability): Evnen til å spore et produkt eller en ingrediens gjennom alle stadier av produksjon, prosessering og distribusjon.

Vesentlig hendelse: En hendelse som har forårsaket eller kan forårsake alvorlig drifts-forstyrrelse eller betydelig økonomisk tap, eller som har påvirket eller kan påvirke andre personer ved å forårsake betydelig skade. Slike hendelser utløser rapporteringsplikt under NIS2.

Vesentlig virksomhet (Essential Entity): Større virksomheter i kritiske sektorer som er underlagt proaktivt tilsyn under NIS2.

Viktig virksomhet (Important Entity): Mellomstore virksomheter i kritiske eller viktige sektorer som er underlagt reaktivt tilsyn under NIS2.

6. Referanser

- Europaparlaments- og rådsdirektiv (EU) 2022/2555 av 14. desember 2022 om tiltak for et høyt felles cybersikkerhetsnivå i hele Unionen.
- Lov om nasjonal sikkerhet (sikkerhetsloven). LOV-2018-06-01-24.
- Lov om digital sikkerhet (digitalsikkerhetsloven). LOV-2023-12-20-108
- Forskrift om digital sikkerhet (digitalsikkerhetsforskriften). FOR-2025-06-20-1131
- Nasjonal sikkerhetsstrategi (Regjeringen, 2025).
- Nasjonal sikkerhetsmyndighet (NSM). (2025). Risiko 2025: Et sikkert Norge i en usikker verden.

7. Vedlegg

For å gi praktisk støtte i oppfølgingen av tiltakene beskrevet i denne veilederen, er det utarbeidet en rekke sjekklister og maler. Disse tar utgangspunkt i kravene i NIS2 og de spesifikke utfordringene i matbransjen.

Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen

Dette vedlegget inneholder en guide for å vurdere kritikaliteten til en IKT-leverandørs tjeneste. Den bygger på virksomhetens egen konsekvensanalyse (BIA).

Vedlegg B: Standard sjekkliste for risikovurdering av leverandører

En sjekkliste for due diligence av mulige leverandører. Listen dekker generelle risikoområder innen informasjonssikkerhet og OT-sikkerhet. Sjekklisten er ment brukt sammen med virksomhetens eksisterende rammeverk for risikovurdering.

Vedlegg C: Standardiserte krav til kontrakter og vedlegg

Dette vedlegget inneholder konkrete kravpunkter som kan inkluderes i kontrakter med IKT-leverandører for å sikre etterlevelse av NIS2 Artikkel 21. Punktene dekker alt fra sikkerhetstiltak og revisjonsrettigheter til håndtering av underleverandører og hendelsesrapportering.

Vedlegg D: Sjekkliste for oppfølging av IKT-leverandører

En sjekkliste strukturert etter en strategisk, taktisk og operasjonell modell for kontinuerlig overvåking og styring av leverandørforholdet.

Vedlegg E: Innhold til exitplan

En mal som beskriver de sentrale elementene en omfattende exitplan for en kritisk eller viktig IKT-leverandør bør inneholde, i tråd med kravene til forretningskontinuitet i NIS2.

Vedlegg F: Sjekkliste for exitplan

En detaljert sjekkliste for å verifisere at alle nødvendige vurderinger er gjort ved utarbeidelse av en exitplan.

Vedlegg G: Triggere for iverksettelse av exitplan

En liste med eksempler på hendelser og scenarioer (triggere) som bør utløse en gjennomgang eller iverksettelse av en exitplan, for eksempel vedvarende tjenesteavbrudd, sikkerhetsbrudd eller endringer hos leverandøren.

Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen

Dette vedlegget gir en stegvis veiledning for å vurdere kritikaliteten til en IT- eller OT-leverandør. Vurderingen er basert på virksomhetens egen konsekvensanalyse (BIA). Målet med denne vurderingen er å kategorisere leveransen som ikke-kritisk, betydningsfull eller kritisk/viktig. Denne kategoriseringen vil styre nivået på videre risikovurdering og oppfølging av IKT-leverandøren.

Steg 1: Konsekvensanalyse (BIA)

Før du vurderer kritikaliteten til en spesifikk leveranse, er det en forutsetning at virksomheten har gjennomført en konsekvensanalyse (Business Impact Analysis, BIA) av sine egne forretningsprosesser og tjenester. Denne analysen identifiserer hvilke prosesser som er kritiske for virksomhetens drift og hvilke konsekvenser et avbrudd vil ha.

Sjekkliste for BIA-forståelse:

- Har virksomheten en oppdatert BIA som identifiserer kritiske forretningsprosesser?
- Er de primære og sekundære konsekvensene av et avbrudd i disse prosessene dokumentert (f.eks. økonomisk tap, omdømmetap, brudd på regulatoriske krav, trussel mot liv og helse)?
- Er det definert maksimale akseptable nedetider (Maximum Tolerable Period of Disruption, MTPD) og gjenopprettingsmål (Recovery Time Objective, RTO / Recovery Point Objective, RPO) for kritiske prosesser?

Dersom det ikke er utført en BIA, anbefales det å gjennomføre en slik før vurdering av kritikalitet på leveransen fortsetter.

Steg 2: Vurdering av kritikalitet på leveransen

Kritikaliteten til en IKT-leveranse vurderes ut fra to hovedfaktorer: kritikalitet av den understøttede leveransen og avhengighet av leverandøren.

2.1. Kritikalitet (konsekvensene av et avbrudd)

Vurder hvor kritisk forretningsprosessene som IKT-leverandøren understøtter er. En prosess eller tjeneste er kritisk hvis et avbrudd truer:

- **Forsyningssikkerhet**. Evnen til å levere mat til samfunnet (f.eks. produksjonsstans, distribusjonsforstyrrelser).
- **Matsikkerhet**. Risiko for forurensning, feil ingrediensblanding, brudd i kjølekjeden eller andre forhold som gjør maten utrygg.
- **Regulatorisk etterlevelse**. Evnen til å overholde lovpålagte krav til sporing, dokumentasjon, hygiene etc.
- **Økonomi/Omdømme**. Betydelig økonomisk tap, alvorlig omdømmetap, eller tap av kundetillit.

Tabell 1. Vurdering av kritikalitet

Kritikalitetsnivå	Beskrivelse (eksempler for matbransjen)
Kritisk	Et avbrudd vil ha svært alvorlige konsekvenser for virksomheten, med umiddelbar og alvorlig innvirkning på forsyningssikkerhet, matsikkerhet, regulatorisk etterlevelse, og/eller medføre betydelig økonomisk tap og omdømmetap. Eksempel: Et SCADA-system som styrer produksjonslinjen for melk, der feil kan føre til forurenset melk eller full stans i produksjon.
Betydningsfull	Et avbrudd vil ha alvorlige konsekvenser for virksomheten, med merkbar innvirkning på forsyningssikkerhet, matsikkerhet, regulatorisk etterlevelse, og/eller medføre moderat økonomisk tap og omdømmetap. Eksempel: Et ERP-system som håndterer innkjøp og lagerstyring, der nedetid kan forsinke leveranser av råvarer og dermed redusere produksjonskapasiteten.
Ikke-kritisk	Et avbrudd vil ha begrenset konsekvens for virksomheten, med minimal innvirkning på forsyningssikkerhet, matsikkerhet, regulatorisk etterlevelse, og/eller medføre ubetydelig økonomisk tap og omdømmetap. Eksempel: En leverandør av kontorprogramvare som ikke er direkte knyttet til produksjon eller kritiske forretningsprosesser.

2.2. Avhengighet (om leverandøren kan erstattes)

Vurder hvor lett IKT-leverandøren kan erstattes dersom det oppstår et problem eller samarbeidet avsluttes. Faktorer som påvirker avhengigheten, inkluderer:

- Proprietær teknologi. Bruker leverandøren proprietær teknologi som gjør det vanskelig å bytte?
- Markedstilgjengelighet. Hvor mange alternative leverandører finnes det for denne spesifikke tjenesten/teknologien?
- Kompleksitet ved bytte. Hvor omfattende og tidkrevende vil det være å bytte leverandør (f.eks. migrering av data, integrasjon med eksisterende systemer, opplæring av ansatte)?
- Investeringer. Hvor store investeringer er gjort i leverandørens spesifikke løsning?

Tabell 2. Vurdering av avhengighet

Avhengighetsnivå	Beskrivelse (eksempler for matbransjen)
Høy	Leverandøren er vanskelig å erstatte på grunn av spesialisert teknologi, begrenset markedstilgjengelighet eller høy kompleksitet ved bytte. Et bytte vil kreve betydelige ressurser og tid, med mulige driftsforstyrrelser. Eksempel: En leverandør av en proprietær SCADA-plattform som styrer en hel fabrikk, eller en spesialisert leverandør av sporingsløsninger for en kompleks forsyningskjede.
Medium	Leverandøren kan erstattes, men det vil kreve en viss innsats og tid. Det finnes alternative løsninger i markedet, men overgangen vil innebære moderat kompleksitet og kostnader. Eksempel: En leverandør av et standard ERP-system som krever tilpasning, men hvor det finnes flere konkurrerende systemer og implementeringspartnere.
Lav	Leverandøren er lett å erstatte. Tjenesten er standardisert, og det finnes mange alternative leverandører i markedet. Bytte vil ha minimal innvirkning på drift og kreve få ressurser. Eksempel: En leverandør av en standardisert skytjeneste for e-post eller generell kontorprogramvare.

Steg 3: Kategorisering av leveransen

Vurder kritikalitet og avhengighet for å fastslå hvor høy prioritet leveransen skal gis i den videre oppfølgingen. Tabellen under er et eksempel, og det forutsettes at virksomheten selv vekter faktorene kritikalitet og avhengighet.

Tabell 3. Eksempel på kategorisering av leveransen

Kategorisering av leveransen **Prioriteten er en vekting av kritikalitet og avhengighet**		**Kritikalitet**		
		Kritisk	**Betydningsfull**	**Ikke-kritisk**
Avhengighet	**Høy**	Høy prioritet	Høy prioritet	Høy prioritet
	Medium	Høy prioritet	Høy prioritet	Medium prioritet
	Lav	Høy prioritet	Medium prioritet	Lav prioritet

- **Høy prioritet.** Krever tettere samarbeid med leverandøren, grundig risikovurdering, omfattende kontraktskrav og kontinuerlig, detaljert oppfølging. Kan innebære krav om uavhengige revisjoner og spesifikke sikkerhetssertifiseringer (f.eks. ISO 27001). Alternative leverandører skal identifiseres og exit-plan skal utarbeides.
- **Medium prioritet.** Kvartalsvis oppfølging av leverandør og avtaler. Vurder behovet for exit-plan og uavhengige revisjoner.
- **Lav prioritet.** Årlig oppfølging av leverandør og avtaler. Øvrig oppfølging kan være behovsbasert.

Steg 4: Dokumentasjon og revisjon

Dokumenter alltid vurderingen av kritikalitet og begrunnelsen for kategoriseringen. Denne dokumentasjonen bør være tilgjengelig for revisjon og oppdateres jevnlig, spesielt ved endringer i leveransens omfang, virksomhetens prosesser eller trusselbildet.

Sjekkliste for dokumentasjon og revisjon:

- Er kritikalitetsvurderingen dokumentert?
- Er begrunnelsen for kategoriseringen tydelig beskrevet?
- Er det etablert en prosess for regelmessig gjennomgang og oppdatering av kritikalitetsvurderingene (f.eks. årlig eller ved vesentlige endringer)?
- Er vurderingen forankret hos relevant ledelse og fagansvarlige?

Eksempel på utfylling:

Leveranse: Vedlikehold og support av SCADA-system for produksjonslinje for meieriprodukter.

1. Kritikalitet (konsekvens av avbrudd):

- **Matsikkerhet:** Høy risiko for feilblanding av ingredienser, brudd i kjølekjeden, og dermed utrygge produkter.
- **Forsyningssikkerhet:** Full stans i produksjon av essensielle varer som melk og yoghurt.
- **Regulatorisk etterlevelse:** Manglende sporbarhet og dokumentasjon av produksjonsprosessen.
- **Økonomi/Omdømme:** Betydelig økonomisk tap og alvorlig omdømmetap ved tilbakekalling av produkter.
- **Konsekvensnivå samlet:** Kritisk.

2. Avhengighet (lett å erstatte):

- **Proprietær teknologi:** SCADA-systemet er en proprietær plattform med få alternative leverandører.
- **Kompleksitet ved bytte:** Bytte av system vil kreve omfattende investeringer, lang implementeringstid og risiko for produksjonsstans under overgangen.
- **Markedstilgjengelighet:** Begrenset antall spesialiserte leverandører med kompetanse på dette spesifikke systemet.
- **Avhengighetsnivå samlet:** Høy.

3. Kategorisering:

- Basert på matrisen (Kritisk konsekvens + Høy avhengighet) kategoriseres denne leveransen som **Høy prioritet**.

4. Videre oppfølging:

- Krever umiddelbar og grundig risikovurdering av leverandøren.
- Kontrakten må inneholde svært detaljerte sikkerhetskrav, SLA-er og varslingsrutiner i tråd med NIS2 Artikkel 21 og 23.
- Kontinuerlig og detaljert oppfølging, inkludert krav om uavhengige revisjoner (f.eks. SOC 2 Type 2 eller lignende).
- Utarbeidelse av en robust exit plan med fokus på overføring av OT-spesifikk kunnskap og systemer.

Vedlegg B: Standard sjekkliste for risikovurdering av IKT-leverandører

Dette vedlegget er ment som et praktisk verktøy til bruk i risikovurdering av leverandører.

En forutsetning for bruk av denne sjekklisten er at virksomheten allerede har gjennomført en grundig kritikalitetsvurdering av den aktuelle leveransen. Denne vurderingen er beskrevet i «Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen». En annen forutsetning er at virksomheten har et rammeverk for risikovurdering, og at denne sjekklisten benyttes i samspill med dette rammeverket.

Dybden og omfanget av risikovurderingen som utføres ved hjelp av denne sjekklisten, skal være direkte proporsjonal med kritikalitetsnivået (Høy prioritet, Medium prioritet, Lav prioritet) som ble fastsatt i Vedlegg A. Dette sikrer en risikobasert tilnærming, og at fokuset rettes mot de områdene som representerer størst risiko for virksomheten.

I dette vedlegget er det foreslått mange krav, og det kan være tid- og ressurskrevende å gjennomføre en god vurdering av disse. Virksomheten må derfor gjøre en innledende vurdering av hvilke krav som er nødvendig å stille til den enkelte leverandør.

1. NIS2-krav (Artikkel 21 og 23)

NIS2 Artikkel 21 (Art.21(2)) omhandler følgende krav til risikostyringstiltak.

Tabell 4. Krav i Art.21(2)

Pkt.	Krav
a)	Retningslinjer for risikoanalyse og informasjonssystemsikkerhet.
b)	Hendelseshåndtering.
c)	Forretningskontinuitet, som backup-håndtering og katastrofegjenoppretting, og krisehåndtering.
d)	Sikkerhet i leverandørkjeden, inkludert sikkerhetsaspekter ved forholdet mellom hver enhet og dens direkte leverandører.
e)	Sikkerhet ved anskaffelse, utvikling og vedlikehold av nettverks- og informasjonssystemer, inkludert sårbarhetshåndtering.
f)	Retningslinjer og prosedyrer for å vurdere effektiviteten av risikostyringstiltakene for cybersikkerhet.
g)	Grunnleggende praksis for cyberhygiene og opplæring i cybersikkerhet.
h)	Retningslinjer og prosedyrer for bruk av kryptografi og, der det er hensiktsmessig, kryptering.
i)	Personellsikkerhet, retningslinjer for tilgangskontroll og kapitalforvaltning (asset management).
j)	Bruk av flerfaktorautentisering (MFA) eller kontinuerlige autentiseringsløsninger, samt sikret tale-, video- og tekstkommunikasjon.

Kontrakter med IKT-leverandører må ta inn disse risikostyringstiltakene og gi virksomheten rett til å vurdere og revidere leverandørens sikkerhetspraksis. De må også kunne gi leverandøren anledning til å kreve forbedringer ved avvik. I tillegg til disse kravene, kan virksomheten velge å inkludere andre krav basert på annet lovverk eller beste praksis.

NIS2 Artikkel 23 omhandler strenge og trinnvise rapporteringsplikter for betydelige sikkerhets-hendelser. En virksomhet må gi et tidlig varsel til nasjonale myndigheter innen 24 timer etter at den er blitt klar over en betydelig hendelse. Dette etterfølges av et mer detaljert hendelsesvarsel innen 72 timer, som skal inneholde en «innledende vurdering, inkludert alvorlighetsgrad og innvirkning».

2. Standard sjekkliste for risikovurdering av IKT-leverandører

Denne sjekklisten er utformet for å veilede virksomheter i matbransjen gjennom en grundig vurdering av IKT-leverandørens styringssystem for informasjonssikkerhet. Dybden av vurderingen bør tilpasses kritikalitetsnivået som er fastsatt i Vedlegg A. For leverandører kategorisert som «Høy prioritet» er en omfattende gjennomgang av alle punkter essensiell, og det bør kreves uavhengige attestasjoner og detaljert dokumentasjon. For «Medium prioritet» kan en mer fokusert gjennomgang av nøkkelområder være tilstrekkelig, med mindre strenge krav til dokumentasjon. For «Lav prioritet» leverandører kan en overordnet gjennomgang eller selvvurdering være tilstrekkelig.

Sjekklisten er strukturert med kolonner for

- Risikoområde
- Vurderingspunkt
- Beskrivelse/eksempel
- Krav til dokumentasjon/bevis

For hvert av de aktuelle risikoområdene bør virksomheten dokumentere sin vurdering (f.eks. Oppfyller, Delvis oppfyller, Oppfyller ikke, Ikke relevant), eventuelle kommentarer/avvik og anbefalte tiltak.

Dette formatet sikrer en systematisk tilnærming til vurderingen og gir rom for detaljert dokumentasjon av funn og foreslåtte tiltak.

Tabell 5. Sjekkliste for risikovurdering av leverandør

Risikoområde	Vurderingspunkt	Beskrivelse/Eksempel	Krav til dokumentasjon/bevis
I. OT-Sikkerhet	Har leverandøren dokumenterte prosesser for sikker utvikling, patching og sårbarhetshåndtering for sitt OT-utstyr og programvare?	Gjelder for systemer som SCADA, PLS, produksjonsstyrings-systemer (MES) og andre systemer som direkte påvirker fysisk produksjon eller matsikkerhet.	Utviklingspolicyer, patchrutiner, sårbarhetsrapporter og testrapporter.
	Beskytter leverandøren det fysiske miljøet til OT-systemene?	Fysisk tilgangskontroll til utstyr, miljøkontroller (temperatur, fuktighet), brannsikring for serverrom/kontrollrom.	Fysiske sikkerhetspolicyer, adgangslogger, bilder/video av sikkerhetstiltak.
	Er det etablert nettverkssegmentering mellom IT- og OT-nettverk?	Vurder om leverandørens løsninger støtter eller krever adskillelse for å minimere angrepsflaten mellom administrative systemer og produksjonssystemer.	Nettverksarkitektur-diagrammer, segmenteringspolicyer, brannmurregler.
	Sikrer leverandøren integriteten til industrielle kontrollsystemer (ICS)?	Tiltak mot uautoriserte endringer i konfigurasjoner, firmware eller programvare som kan påvirke produksjonskvalitet eller -sikkerhet.	Endringskontrollprosedyrer, integritetskontroller, revisjonslogger.
II. Sikker fjerntilgang	Benyttes flerfaktor-autentisering (MFA) for all fjerntilgang?	Spesielt kritisk for teknikere som får fjerntilgang til produksjonssystemer eller sensitive data.	MFA-policy, konfigurasjonsbevis og tilgangslogger.
	Benyttes kontrollerte tilgangspunkter («jump hosts») og tidsbegrenset, overvåket tilgang for vedlikeholds-personell?	Reduserer risikoen for direkte eksponering av OT-nettverk.	Tilgangspolicyer, loggingsrutiner, overvåkingsrapporter.
	Er tilgangen basert på prinsippet om minst privilegium (Least Privilege)?	Sikrer at leverandørens personell kun har tilgang til det absolutt nødvendige for å utføre sine oppgaver.	Tilgangsmatriser, rollebasert tilgangskontroll (RBAC) dokumentasjon.

	Logges og overvåkes all fjerntilgang?	For å kunne spore aktivitet, oppdage uregelmessigheter og utføre revisjoner.	Revisjonslogger, SIEM-integrasjon, overvåkingsrapporter.
III. Leverandør-kjedesikkerhet	Har leverandøren oversikt over og stiller sikkehetskrav til sine egne kritiske underleverandører?	Gjelder f.eks. leverandører av programvarekomponenter, maskinvare, skytjenester eller spesialiserte tjenester som påvirker leveransen til din virksomhet (NIS2 Artikkel 21(2)(d)).	Underleverandøroversikt, kontrakter med underleverandører, underleverandør-revisjonsrapporter.
	Kan leverandøren fremvise en «Software Bill of Materials» (SBOM) eller tilsvarende for programvarekomponenter?	For å identifisere og håndtere sårbarheter i tredjeparts-komponenter.	SBOM-dokumentasjon, lister over avhengigheter.
	Har leverandøren en etablert prosess for risikostyring av sin egen leverandør-kjede?	Inkluderer vurdering, oppfølging og risikoreduksjon for underleverandører.	Leverandørkjede-risikostyringspolicyer, prosessbeskrivelser.
IV. Informasjons-sikkerhet (Generelt)	Har leverandøren et etablert styringssystem for informasjons-sikkerhet (ISMS)?	F.eks. basert på ISO 27001, NIST Cybersecurity Framework, eller tilsvarende anerkjente standarder.	ISMS-dokumentasjon, sertifikater og policyer.
	Hvordan håndteres datasikkerhet, personvern og tilgangskontroll?	Inkluderer kryptering, dataminimering, tilgangsstyring, og etterlevelse av GDPR (hvis relevant).	Databehandleravtaler, krypteringspolicyer, tilgangsstyringsprosedyrer.
	Har leverandøren prosesser for sårbarhetshåndtering og sikker utvikling av programvare?	Inkluderer regelmessig sårbarhetsskanning, penetrasjonstesting, og gjennomgang av DevSecOps-praksiser.	Sårbarhetshåndteringspolicy, testrapporter, utviklingsstandarder.
	Har leverandøren gitt ansatte og innleide tilstrekkelig opplæring i cybersikkerhet?	Spesielt for teknikere som jobber i kundens fysiske eller digitale miljø.	Opplæringsplaner og kompetanseoversikter.
	Har leverandøren en robust løsning for sikkerhets-kopiering og gjenoppretting av data?	For å sikre kontinuitet og dataintegritet ved hendelser.	Backup-policy, gjenopprettingstester, Recovery Time Objective/Recovery Point Objective.
V. Hendelses-håndtering og rapporteringsplikt	Har leverandøren en dokumentert plan for hendelseshåndtering?	Inkluderer deteksjon, analyse, håndtering, gjenoppretting og etteranalyse.	Hendelseshåndteringsplan, responsprosedyrer.
	Forstår leverandøren sin rolle og sine forpliktelser i kundens rapporteringsplikt under NIS2 Artikkel 23?	Inkluderer forståelse for tidsfrister for varsling til din virksomhet, som må være kortere enn dine egne frister til myndighetene.	Kontraktsfestede varslingsfrister (SLA), bevisstgjøringsmateriell om NIS2.
	Er det avtalt klare kommunikasjonskanaler og varslingsrutiner for sikkerhets-hendelser?	Sikrer rask og effektiv informasjonsflyt mellom leverandør og din virksomhet.	Kommunikasjonsplan, varslingsprosedyrer.

	Gjennomfører leverandøren regelmessige øvelser for hendelseshåndtering?	For å teste og forbedre responsplanene.	Øvelsesrapporter, forbedringstiltak.
VI. Forretnings-kontinuitet og exit-strategi	Har leverandøren en etablert plan for forretningskontinuitet og katastrofegjenoppretting (Business Continuity Plan/ Disaster Recovery Plan)?	For å sikre kontinuitet i leveransen ved større forstyrrelser.	BCP/DRP-dokumentasjon, testrapporter.
	Kan leverandøren demonstrere evne til å sikre kontinuitet i kritiske funksjoner under en overgangsperiode?	Spesielt relevant for OT-systemer hvor bytte av leverandør er komplekst og tidkrevende.	Overgangsplaner, transisjons- og migrasjonsstrategier.
	Er det en klar exit-strategi for leveransen, spesielt for kritiske/ viktige IKT-leverandører?	Inkluderer overføring av data, systemer og kompetanse.	Exit-plan, prosedyre for dataoverføring/sletting, kunnskapsoverføringsplan.
VII. Finansiell stabilitet	Er leverandøren økonomisk stabil nok til å garantere langsiktig leveranse og support?	Spesielt viktig for systemer med lang levetid, som OT-utstyr, hvor bytte er kostbart og komplekst.	Årsregnskap, kredittvurderinger, revisjonsrapporter.
VIII. Revisjon og uavhengige attestasjoner	Er leverandøren villig til å gjennomgå revisjoner eller sikkerhetsvurderinger utført av din virksomhet eller en uavhengig tredjepart?	For å verifisere etterlevelse av avtalte sikkerhetskrav.	Revisjonsrettigheter i kontrakt, tidligere revisjonsrapporter.
	Kan leverandøren fremvise uavhengige attestasjoner av internkontrollen (f.eks. ISO 27001, SOC 2 Type 2)?	Gir en uavhengig vurdering av leverandørens sikkerhetskontroller.	Sertifikater, SOC 2-rapporter, ISAE 3402-rapporter.
	Har leverandøren en prosess for å håndtere og lukke avvik identifisert i revisjoner/ attestasjoner?	Sikrer at funn følges opp med korrigerende tiltak.	Avvikshåndteringsprosedyrer, oversikt over lukkede avvik.
IX. Konsentrasjons-risiko	Har virksomheten en høy grad av avhengighet til én enkelt leverandør for flere kritiske funksjoner?	Intern konsentrasjonsrisiko. Det kan for eksempel være om den samme leverandøren leverer skytjenester, ERP-systemer, og produksjonsstyringssystemer. En feil eller et cyberangrep hos denne ene leverandøren vil da kunne slå ut flere kritiske forretningsprosesser samtidig.	Oversikt over alle tjenester som leveres av leverandøren. Analyse av leverandørens rolle i de ulike forretningsprosessene. Vurdering av konsekvensene ved et samlet utfall av disse tjenestene.
	Hvor mange andre virksomheter i samme bransje bruker den samme leverandøren eller en tilsvarende teknologi?	Ekstern konsentrasjons-risiko. Hvis mange virksomheter i matbransjen benytter den samme leverandøren for kritiske OT-systemer, kan et cyberangrep på denne leverandøren potensielt ramme hele bransjen. Dette kan føre til en systemisk risiko som påvirker forsyningssikkerheten i samfunnet.	Bransjeanalyser, informasjon fra bransjeorganisasjoner, og offentlig tilgjengelig informasjon om leverandørens kundebase.

Hvilke planer har virksomheten for å redusere konsentrasjons-risikoen?	Vurderer hvilke strategier virksomheten har for å redusere risikoen. Dette kan inkludere å ha alternative leverandører, diversifisere teknologien som brukes, eller utvikle interne løsninger for kritiske prosesser.	Strategiske planer for leverandør-styring, oversikt over alternative leverandører, og beredskapsplaner for overgang til andre løsninger ved en eventuell leverandørsvikt.

3. Veiledning for bruk av sjekklisten

Etter å ha gjennomført risikovurderingen ved hjelp av sjekklisten, er det viktig å tolke resultatene og prioritere risikoreduserende tiltak på en strukturert måte. Vurderingene bør aggregeres for å identifisere den samlede risikoeksponeringen. Anbefalte tiltak bør prioriteres basert på leveransens kritikalitet (som ble fastsatt i Vedlegg A) og alvorlighetsgraden av de identifiserte avvikene.

Oppfølging av risikoreduserende tiltak bør integreres i virksomhetens eksisterende rammeverk og prosess for risiko- og leverandørstyring.

Identifiserte mangler og risikoer bør oversettes til konkrete kontraktsmessige krav, servicenivåavtaler (SLAer) og rettigheter til å utføre revisjoner, i tråd med NIS2 Artikkel 21(2)(d). Denne sjekklisten kan også fungere som et levende dokument som danner grunnlaget for kontinuerlig overvåking og oppfølging gjennom hele leverandørens livssyklus. Regelmessige gjennomganger, ytelsesrapporter og re-vurderinger bør utføres, spesielt for kritiske leverandører for å sikre at sikkerhetsnivået opprettholdes over tid. Dette inkluderer oppfølging av uavhengige vurderinger som for eksempel ISO 27001-sertifiseringer eller SOC 2-rapporter.

Dokumentasjon og regelmessig revisjon er svært viktig. Dokumentasjon av risikostyringsprosesser, og alle vurderinger, funn og iverksatte tiltak må dokumenteres og være lett tilgjengelige for revisjoner. Det er viktig med periodisk gjennomgang og oppdatering av leverandørrisikovurderingene, spesielt etter betydelige hendelser, endringer i leverandørtjenester, eller oppdateringer av regulatoriske krav, for å sikre at de forblir relevante og effektive.

Vedlegg C: Standardiserte krav til kontrakter og vedlegg

Dette vedlegget har eksempler på standardiserte krav som kan inkluderes i kontrakter og tilhørende vedlegg med IKT-leverandører. Formålet er å sikre et tydelig og juridisk bindende grunnlag for sikkerhetsarbeidet gjennom hele leverandørforholdets livssyklus.

Valget mellom å bruke «skal» og «bør» i kontraktsmessige krav er av stor betydning. «Skal» innebærer normalt et absolutt og ufravikelig krav, mens «bør» representerer en sterk anbefaling eller beste praksis som kan være gjenstand for diskusjon basert på en risikovurdering. I dette vedlegget er kravene formulert med «skal» for å understreke at de utgjør et anbefalt utgangspunkt for de mest kritiske leveransene. I den endelige kontrakten må virksomheten, basert på en konkret risikovurdering av den enkelte leveranse, avgjøre hvilke punkter som skal være absolutte krav («skal») og hvilke som kan formuleres som anbefalinger («bør»).

Kravene er laget for å være konkrete og målbare, og de dekker sentrale områder som generell informasjonssikkerhet, sikkerhet i leverandørkjeden, håndtering av operasjonell teknologi (OT), hendelsesrapportering, revisjonsrettigheter og forretningskontinuitet. For hvert krav er det spesifisert et tilhørende dokumentasjonskrav som leverandøren må kunne fremlegge for å verifisere etterlevelse. Virksomheten må selv vurdere hvilke krav som er relevante for den enkelte leveranse, basert på leveransens kritikalitet (se Vedlegg A).

1. Generell informasjonssikkerhet og styring

Tabell 6. Eksempel på generelle krav innen informasjonssikkerhet og styring

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
1.1	**Styringssystem for informasjonssikkerhet (ISMS)** Leverandøren skal ha etablert, implementert og vedlikeholdt et styringssystem for informasjonssikkerhet basert på en anerkjent standard (f.eks. ISO/IEC 27001 eller tilsvarende).	Gyldig sertifikat (f.eks. ISO/IEC 27001) eller uavhengig revisjonsrapport (f.eks. ISAE 3402, SOC 2). Alternativt: Policyer, prosedyrer og annen dokumentasjon fra ISMS.	
1.2	**Risikostyring** Leverandøren skal årlig gjennomføre og dokumentere risikovurderinger av egne systemer og tjenester som omfattes av avtalen. Vesentlige risikoer skal følges opp med tiltaksplaner.	Dokumenterte risikovurderinger og tilhørende tiltaksplaner.	
1.3	**Kompetanse og bevisstgjøring** Leverandøren skal sikre at alt personell med tilgang til virksomhetens data eller systemer har gjennomført sikkerhetsopplæring.	Dokumentasjon på gjennomført opplæringsprogram, inkludert innhold og deltakerlister.	
1.4	**Sikker utvikling** All programvare som utvikles eller leveres under avtalen skal følge prinsipper for sikker utvikling (f.eks. OWASP Top 10, DevSecOps-prinsipper).	Policy for sikker utvikling. Resultater fra sikkerhetstesting (f.eks. SAST, DAST, penetrasjonstester).	
1.5	**Sårbarhetshåndtering** Leverandøren skal ha en dokumentert prosess for å identifisere, vurdere og utbedre sårbarheter i systemer som omfattes av avtalen, i henhold til avtalte tidsfrister (SLA).	Policy for sårbarhetshåndtering. Rapporter fra sårbarhetsskanninger og oversikt over lukkede sårbarheter (patch-rapporter).	

1.6	**Kryptering** Data under overføring (in transit) og ved lagring (at rest) skal som et minimum krypteres i henhold til anerkjent bransjestandard.	Policy for kryptering. Teknisk dokumentasjon eller konfigurasjonsuttrekk som bekrefter bruk av kryptering.
1.7	**Tilgangskontroll** Tilgang til virksomhetens data og systemer skal være basert på prinsippene om «need-to-know» og «least privilege». Flerfaktorautentisering (MFA) skal benyttes for all fjerntilgang og for tilgang til kritiske systemer.	Policy for tilgangskontroll. Tilgangsmatrise som viser roller og rettigheter. Teknisk bevis på implementert MFA.
1.8	**Dataformater** Data skal lagres på formater som muliggjør effektiv og rask overføring av data fra leverandøren til virksomheten	Dokumentasjon på hvilke data-formater som brukes og hvordan disse kan overføres til virksomheten.

2. Sikkerhet i leverandørkjeden

Tabell 7. Eksempel på krav innen sikkerhet i leverandørkjeden

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
2.1	**Kontroll på underleverandører** Leverandøren skal ha en oppdatert oversikt over alle under-leverandører som benyttes for å levere tjenesten. Leverandøren er fullt ut ansvarlig for at underleverandører etterlever sikkerhetskravene i denne avtalen.	Oppdatert liste over under-leverandører. Kontraktsmaler eller klausuler som viser at sikkerhetskrav er videreført. Resultater fra revisjoner av underleverandører.	
2.2	**Informasjonsplikt** Leverandøren plikter å informere virksomheten umiddelbart ved bytte av eller inngåelse av avtale med ny kritisk underleverandør. Virksomheten har rett til å motsette seg bruk av underleveran-dører som ikke møter avtalte sikkerhetskrav.	Skriftlig varsel om endringer i underleverandørkjeden.	
2.3	**«Software Bill of Materials» (SBOM)** For all programvare levert under avtalen, skal leverandøren på forespørsel kunne fremlegge en SBOM for å muliggjøre identifisering av sårbarheter i tredjepartskomponenter.	SBOM-dokumentasjon i et standardformat (f.eks. SPDX, CycloneDX).	

3. Sikkerhet for operasjonell teknologi (OT)

Tabell 8. Eksempel på krav innen OT

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
3.1	**Nettverkssegmentering** Leverandørens løsninger skal understøtte og ikke hindre nettverkssegmentering mellom IT- og OT-miljøer hos virksomheten. All kommunikasjon mellom sonene skal være strengt kontrollert.	Nettverksarkitektur-diagrammer. Dokumentasjon på konfigurasjon av brannmurer eller andre sikkerhetskontroller.	
3.2	**Sikker fjerntilgang til OT** All fjerntilgang til OT-systemer skal skje via en sikker, overvåket og tidsbegrenset løsning (f.eks. «jump host»). Tilgangen skal logges, og MFA er nødvendig.	Policy for sikker fjerntilgang til OT. Tilgangslogger som viser tidspunkt, bruker og aktivitet.	
3.3	**Fysisk sikkerhet** Leverandøren plikter å følge virksomhetens retningslinjer for fysisk sikkerhet ved arbeid i produksjonsområder eller andre sikrede soner.	Bekreftelse på at retningslinjer er mottatt og forstått.	

4. Teknisk sammenkobling og integrasjon

Tabell 9. Eksempel på krav innen teknisk sammenkobling og integrasjon

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
4.1	**API-sikkerhet** Alle API-er som benyttes for integrasjon skal være sikret i henhold til beste praksis (f.eks. OAuth 2.0, TLS) og ha rate limiting for å forhindre misbruk.	API-dokumentasjon som beskriver sikkerhetsmekanismer. Konfigurasjonsbevis for rate limiting og autentisering.	
4.2	**Endringsstyring for integrasjoner** Leverandøren skal varsle virksomheten minimum [f.eks. 60] dager i forkant av planlagte endringer i API-er eller andre integrasjonspunkter som kan påvirke virksomhetens systemer.	Endringslogg for API-er. Skriftlig varsel om kommende endringer.	
4.3	**Logging og overvåking** All trafikk og alle kall gjennom integrasjonspunkter skal logges. Loggene skal inneholde tilstrekkelig informasjon for feilsøking og sikkerhetsovervåking.	Policy for logging. Eksempler på logger. Dokumentasjon på hvordan virksomheten kan få tilgang til logger.	
4.4	**Dedikerte tjenestekontoer** Alle integrasjoner skal benytte dedikerte tjenestekontoer med minimalt nødvendige rettigheter. Bruk av personlige brukerkontoer for systemintegrasjoner er ikke tillatt.	Oversikt over tjenestekontoer og deres rettigheter. Konfigurasjonsbevis.	
4.5	**Testmiljø** Leverandøren skal stille et stabilt testmiljø (sandkasse) til disposisjon, som er funksjonelt likt produksjonsmiljøet, slik at virksomheten kan utvikle og teste integrasjoner.	Dokumentasjon for testmiljøet, inkludert tilgangsinformasjon og eventuelle begrensninger.	

5. Hendelseshåndtering og rapportering (I tråd med NIS2 Art. 23)

Tabell 10. Eksempel på krav innen hendelseshåndtering og rapportering

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
5.1	**Plan for hendelseshåndtering** Leverandøren skal ha en dokumentert plan og etablerte prosedyrer for å håndtere sikkerhetshendelser.	Hendelseshåndteringsplan. Resultater fra gjennomførte hendelsesøvelser.	
5.2	**Varslingsplikt (SLA)** Leverandøren skal varsle virksomheten uten ugrunnet opphold, og senest innen [f.eks. 12] timer etter å ha blitt klar over en sikkerhetshendelse som påvirker tjenesten.	Hendelseslogg og dokumentasjon på overholdt varslingsfrist.	
5.3	**Bistandsplikt ved hendelse** Ved en sikkerhetshendelse skal leverandøren umiddelbart bistå med nødvendig informasjon for at virksomheten kan overholde sin rapporteringsplikt til myndighetene. Dette inkluderer innledende vurdering av alvorlighetsgrad, innvirkning og tekniske indikatorer (Indicators of Compromise, IoC).	Teknisk rapport etter hendelse. Deltakelse i hendelsesmøter.	
5.4	**Øvelser** Leverandøren skal på forespørsel, og minst årlig, delta i en felles hendelsesøvelse med virksomheten for å teste varslings- og samarbeidsrutiner.	Rapport fra gjennomført øvelse med identifiserte læringspunkter.	

6. Revisjon og kontroll

Tabell 11. Eksempel på krav innen revisjon og kontroll

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
6.1	**Revisjonsrett** Virksomheten, eller en uavhengig tredjepart utpekt av virksomheten, har rett til å gjennomføre revisjon av leverandørens etterlevelse av sikkerhetskravene i denne avtalen, med [f.eks. 30] dagers varsel.	Tilgang til relevant dokumentasjon, systemer og personell under revisjon.	
6.2	**Uavhengige attestasjoner** Leverandøren skal årlig fremlegge uavhengige revisjonsrapporter eller sertifiseringer for tjenesten (f.eks. ISO/IEC 27001, SOC 2 Type II, ISAE 3402).	Kopi av gyldige sertifikater og revisjonsrapporter.	
6.3	**Oppfølging av avvik** Leverandøren skal utarbeide en plan for å lukke alle avvik identifisert i revisjoner innen en avtalt tidsfrist. Fremdrift skal rapporteres til virksomheten.	Avviksrapport med tiltaksplan og status for lukking.	

7. Forretningskontinuitet og exit

Tabell 12. Eksempel på krav innen forretningskontinuitet og exit

Nr.	Krav (Formulering i kontrakt)	Dokumentasjonskrav (Bevis fra leverandør)	Vurdering
7.1	**Forretningskontinuitet (BCP)** Leverandøren skal ha en dokumentert og testet plan for forretningskontinuitet for å sikre leveranse av tjenesten ved alvorlige forstyrrelser.	Plan for forretningskontinuitet (BCP) og katastrofegjenopp-retting (DRP). Rapport fra siste BCP/DRP-test.	
7.2	**Krav til backup** Leverandøren skal utføre jevnlig sikkerhetskopiering av virksomhetens data. Gjenoppretting av data skal testes minst årlig.	Backup-policy. Rapport fra siste gjenopprettingstest.	
7.3	**Bistand ved avslutning (Exit)** Ved avtalens opphør plikter leverandøren å bistå i en overgangsperiode på [f.eks. 90] dager for å sikre en kontrollert overføring av data, systemer og kompetanse til virksomheten eller en ny leverandør. Detaljer spesifiseres i en egen exit-plan.	Signert exitplan.	
7.4	**Overføring av data** Leverandøren skal overføre virksomhetens data når virksomheten ber om det, og selv om det ikke er besluttet en avslutning av leverandørforholdet.	Skriftlig bekreftelse på at data er overført.	
7.5	**Sikker sletting av data** Etter endt overgangsperiode skal leverandøren sikkert og permanent slette alle virksomhetens data fra sine systemer, inkludert sikkerhetskopier.	Skriftlig bekreftelse eller destruksjonssertifikat som attesterer at data er slettet.	

Vedlegg D: Sjekkliste for oppfølging av IKT-leverandører

Dette vedlegget er utformet for å sikre systematisk og kontinuerlig overvåking og styring av IKT-leverandørforhold gjennom hele livssyklusen.

Sjekklisten er strukturert i tre nivåer: strategisk (ledelsesnivå), taktisk (avtalestyring) og operasjonelt (daglig leveranse). Denne inndelingen definerer de ulike ansvarsområdene og den varierende aktivitetsfrekvensen som er nødvendig for en helhetlig styring av leverandørforhold. Hvert nivå omfatter spesifikke sjekkpunkter som skal tilpasses basert på kritikaliteten av leveransen, som er definert i «Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen».

Utgangspunktet i kritikalitet muliggjør en risikobasert tilnærming i oppfølgingen. Dybden og frekvensen av oppfølgingen skal være direkte proporsjonal med kritikalitetsnivået, slik at oppfølgingen rettes mot de områdene som representerer størst risiko for virksomhetens drift. I en kompleks forsyningskjede utgjør ikke alle leverandører den samme risikoen. Ved å koble oppfølgingsintensiteten til leveransens kritikalitet, kan virksomheten få en mer effektiv utnyttelse av begrensede sikkerhets- og styringsressurser.

Sjekklisten fremhever spesielt NIS2 Artikkel 21 om risikostyringstiltak (inkludert leverandørkjedesikkerhet og forretningskontinuitet) og Artikkel 23 om rapporteringsplikt ved hendelser.

1. Strategisk nivå (Ledelsesnivå)

Dette nivået fokuserer på ledelsens overordnede ansvar for å etablere et robust rammeverk for leverandørrisikostyring, overvåke den samlede risikoprofilen og sikre strategisk forankring av disse prosessene. Oppfølgingen på dette nivået er typisk årlig eller ved behov.

1.1. Overordnet ansvar og styring av leverandørrisiko

Det er viktig at ledelsen etablerer en strategi og policy for styring av IKT-leverandørrisiko, og at denne er forankret i virksomhetens overordnede risikostyringsrammeverk. Ledelsen må definere klare ansvarsområder og roller på tvers av organisasjonen for å sikre en helhetlig tilnærming til risikostyring på dette området.

1.2. Gjennomgang av samlet risikoprofil for IKT-leverandører

Ledelsen skal jevnlig gjennomgå den samlede risikoprofilen for kritiske og viktige IKT-leverandører. Dette omfatter en vurdering av aggregerte funn fra risikovurderinger, identifiserte avvik og status for iverksatte risikoreduserende tiltak. En viktig del av dette er også å vurdere risiko knyttet til underleverandører i hele verdikjeden.

Ledelsen må sørge for at det blir etablert prosesser for å identifisere og vurdere nye eller endrede risikoer knyttet til leverandørkjeden, både for operasjonell teknologi (OT)-systemer og IT-tjenester.

1.3. Sikring av NIS2-samsvar på ledelsesnivå

Ledelsen må sikre at kontrakter med IKT-leverandører reflekterer risikostyringstiltakene som kreves i NIS2 Artikkel 21. Disse kontraktene er ikke lenger kun kommersielle avtaler, de er nå sentrale styringsdokumenter for sikkerhet. De må gi virksomheten rett til å vurdere og revidere leverandørens sikkerhetspraksis og kreve forbedringer ved avvik. Dette inkluderer også krav til leverandørens håndtering av egne underleverandører.

Videre må det etableres en overordnet plan for hendelseshåndtering som sikrer overholdelse av NIS2 Artikkel 23s rapporteringsplikter. Ledelsen må være klar over at forsinkelser hos en leverandør direkte kan føre til at egen virksomhet bryter bestemmelsene i NIS2 Artikkel 23, og sørge for at kontraktsfestede servicenivåavtaler (SLAer) for hendelsesvarsling er på plass. Disse må også regelmessig testes og forstås likt av begge parter.

1.4. Oppfølging av revisjonsfunn

Ledelsen skal jevnlig vurdere uavhengige revisjoner, som ISO 27001-sertifiseringer, SOC 2-rapporter eller ISAE 3402-rapporter, for kritiske og viktige leverandører. Slike rapporter gir en uavhengig vurdering av leverandørens internkontroll og kan bekrefte samsvar med NIS2-kravene. Det skal også etableres en prosess for å sikre at avvik identifisert i disse uavhengige vurderingene følges opp med tilstrekkelige korrigerende tiltak av leverandøren.

Tabell 13. Strategiske sjekkpunkter for ledelsesnivået

Sjekkpunkt	Beskrivelse	Frekvens (Minimum)	Ansvarlig	Dokumentasjon/ Bevis	Kritikalitet (H/M/L)
Overordnet strategi og policy	Er det en godkjent strategi for leverandørrisikostyring?	Årlig	Ledelsen	Strategi-dokument, policy	H
Samlet risikoprofil	Gjennomgang av aggregerte risikoer fra kritiske leverandører.	Halvårlig/ Årlig	Ledelsen	Risikorapporter, styremøtereferater	H
NIS2 Artikkel 21-samsvar	Verifisering av at kontrakter gir tilstrekkelige rettigheter og krav.	Årlig	Ledelsen, Juridisk	Kontraktsmaler, revisjonsrettigheter	H
NIS2 Artikkel 23-samsvar	Sikring av overordnet beredskapsplan for hendelsesrapportering.	Halvårlig	Ledelsen, Sikkerhets-ansvarlig	Beredskapsplan, øvelsesrapporter	H
Oppfølging av attestasjoner	Gjennomgang av uavhengige revisjonsrapporter (SOC 2, ISO 27001).	Årlig	Ledelsen, Internrevisjon	Attestasjoner, avvikslogg	H

Denne tabellen inneholder de strategiske ansvarsområdene som konkrete sjekkpunkter for ledelsen. Den tydeliggjør ansvarsfordelingen, gir konkrete retningslinjer for møtefrekvens og spesifiserer hvilken dokumentasjon som kreves som bevis på at tilsynet er utført. Dette sikrer at overordnet styring er dokumentert og reviderbar.

2. Taktisk nivå (Avtalestyring)

Dette nivået har fokus på den periodiske oppfølgingen av kontrakter og servicenivåavtaler (SLAer). Oppfølgingen bør typisk være kvartalsvis eller halvårlig for kritiske og viktige leverandører.

2.1. Kontraktsmessig oppfølging og overholdelse av SLA

Det er nødvendig å gjennomgå leverandørens ytelsesrapporter og overholdelse av avtalte SLAer regelmessig for å sikre at det avtalte sikkerhetsnivået opprettholdes over tid. For kritiske leverandører bør dette være en kontinuerlig prosess. Avvik fra SLAer må følges opp med leverandøren, og det må iverksettes korrigerende tiltak.

2.2. Gjennomgang av leverandørens sikkerhetsstatus

Virksomheten må verifisere leverandørens prosesser for sikkerhet i både IT- og OT-systemer, inkludert sikker utvikling, patching og sårbarhetshåndtering. For leverandører av OT-systemer er det viktig å sikre at de har dokumentert sikkerheten for det som direkte påvirker fysisk produksjon og matsikkerhet.

Det er også viktig å ha oversikt over leverandørens kritiske underleverandører og at det stilles krav til deres sikkerhet i tråd med NIS2 Artikkel 21(2)(d). Sikkerhet i leverandørkjeden er et kjerneelement i NIS2, og virksomheten må sikre at leverandøren har kontroll på sine egne underleverandører.

Leverandørens sårbarhetshåndtering og praksis for sikker utvikling av programvare (DevSecOps) må gjennomgås. Kontrakten skal spesifisere krav til sårbarhetshåndtering og sikker utvikling, og dette er en kontinuerlig oppfølgingsaktivitet.

Generell informasjonssikkerhet hos leverandøren, inkludert datasikkerhet, personvern, tilgangskontroll og bruk av kryptering, må vurderes. Disse grunnleggende sikkerhetstiltakene må være på plass og kontinuerlig overvåkes.

2.3. Håndtering av hendelser og rapporteringsplikt

Det må avtales klare kommunikasjonskanaler og varslingsrutiner for sikkerhetshendelser med leverandøren, og disse må testes regelmessig. Rask og effektiv informasjonsflyt er viktig for å overholde NIS2 Artikkel 23s tidsfrister. Leverandøren skal ha en dokumentert plan for hendelses-håndtering som er integrert med virksomhetens egen plan, og det bør gjennomføres felles øvelser. Hendelseshåndtering er en felles forpliktelse som krever tett koordinering mellom partene.

2.4. Oppfølging av avvik fra revisjoner og uavhengige vurderinger

Avvik identifisert i uavhengige revisjoner og vurderinger (f.eks. SOC 2 eller ISAE 3402) må følges opp med leverandøren for å sikre at korrigerende tiltak iverksettes. Dette er en kontinuerlig prosess for kritiske og viktige leverandører for å sikre at sikkerhetsnivået opprettholdes over tid.

Tabell 14. Taktiske sjekkpunkter for avtalestyring

Sjekkpunkt	Beskrivelse	Frekvens (Minimum)	Ansvarlig	Dokumentasjon/ Bevis	Kritikalitet (H/M/L)
SLA-overholdelse	Gjennomgang av leverandørens ytelsesrapporter og avvik.	Kvartalsvis (H), Halvårlig (M)	Avtaleansvarlig	Ytelsesrapporter, avvikslogg	H, M
OT-sikkerhets-prosesser	Verifisering av sikker utvikling, patching, sårbarhetshåndtering for OT.	Halvårlig (H), Årlig (M)	IT/OT-sikkerhets-ansvarlig	Policyer, testrapporter	H, M
Under-leverandør-kontroll	Gjennomgang av leverandørens oversikt og krav til egne underleverandører.	Halvårlig (H), Årlig (M)	Avtaleansvarlig, Sikkerhets-ansvarlig	Underleverandør-oversikt, kontrakter	H, M
Sårbarhets-håndtering	Oppfølging av leverandørens sårbarhetsskanninger og patching.	Kvartalsvis (H), Halvårlig (M)	IT/OT-sikkerhets-ansvarlig	Sårbarhets-rapporter, patchlogger	H, M
Hendelses-varsling NIS2 Art. 23	Verifisering av varslingsrutiner og tidsfrister for hendelser.	Kvartalsvis (H), Halvårlig (M)	Avtaleansvarlig, Sikkerhets-ansvarlig	Kommunikasjons-plan, testrapporter	H, M
Avvik fra revisjoner	Oppfølging av korrigerende tiltak for avvik i SOC 2/ISO 27001-rapporter.	Kvartalsvis (H), Halvårlig (M)	Internrevisjon, Sikkerhets-ansvarlig	Avvikslogg, statusrapporter	H, M

Denne tabellen inneholder sjekkpunkter for taktisk styring. Disse bidrar til å operasjonalisere kontraktsbestemmelsene, og sikrer at det avtalte sikkerhetsnivået aktivt følges opp.

3. Operasjonelt nivå (Daglig oppfølging)

Dette nivået omfatter de daglige eller rutinemessige aktivitetene for overvåking av tjenesteleveransen og hendelseshåndtering. Oppfølgingen er typisk daglig, ukentlig eller månedlig.

3.1. Kontinuerlig overvåking av tjenesteleveranse og ytelse

Leverandørens systemer og tjenester må overvåkes kontinuerlig for ytelsesavvik, oppetid og ressursbruk. Dette inkluderer daglig gjennomgang av logger og automatiserte varsler for å identifisere mulige problemer. Aktivitetsdata, dataintegritet og sporbarhet for data som behandles av leverandøren, spesielt for produksjons- og matsikkerhetsdata, må kunne overvåkes og verifiseres.

3.2. Operasjonell hendelseshåndtering og varslingsrutiner

Det er nødvendig å etablere og øve på rutiner for umiddelbar varsling fra leverandøren ved sikkerhets-hendelser eller driftsforstyrrelser. Hurtig respons er viktig for å overholde NIS2 Artikkel 23s krav om tidlig varsel, innen 24 timer etter at virksomheten blir klar over en betydelig hendelse. Første respons og innledende informasjonsutveksling må avtales på forhånd og koordineres tett med leverandøren ved en hendelse. Dette kan bidra til en rask og nøyaktig innledende vurdering innen 72 timer, slik NIS2 krever.

3.3. Sikker operasjonell praksis for IT- og OT-systemer

Logger for all fjerntilgang utført av leverandørens personell, spesielt til OT-nettverk, må overvåkes for uautorisert aktivitet. Dette inkluderer å sjekke for bruk av flerfaktorautentisering (MFA), bruk av kontrollerte tilgangspunkter («jump hosts») og overholdelse av prinsippet om minst privilegium og annen relevant aktivitet. Regelmessig logganalyse fra både IT- og OT-systemer som leverandøren drifter eller har tilgang til, må gjennomføres for å kunne oppdage uregelmessigheter og forsøk på sikkerhetsbrudd.

Videre må leverandørens sårbarhetsskanninger og patching-aktiviteter for OT-utstyr og programvare følges rutinemessig opp. Dette er viktig for å redusere angrepsflaten i industrielle kontrollsystemer og virksomhetens øvrige IKT-struktur. Fysiske sikkerhetstiltak knyttet til OT-systemer som leverandøren vedlikeholder, for eksempel adgangskontroll til serverrom eller produksjonsområder, må kontrolleres. NIS2 Artikkel 21 krever beskyttelse av både nettverk og det fysiske miljøet til disse systemene.

Tabell 15. Operasjonelle sjekkpunkter for kontinuerlig oppfølging

Sjekkpunkt	Beskrivelse	Frekvens (Minimum)	Ansvarlig	Dokumentasjon/ Bevis	Kritikalitet (H/M/L)
Ytelsesovervåking	Daglig gjennomgang av systemlogger og varsler for ytelsesavvik.	Daglig (H), Ukentlig (M), Månedlig (L)	IT/OT-drift	Overvåkings-rapporter, varslingslogg	H, M, L
Dataintegritet/ sporbarhet	Rutinemessige kontroller av dataintegritet og sporbarhetssystemer.	Daglig (H), Ukentlig (M)	Kvalitet/ Produksjon, IT/OT-drift	Dataverifiserings-logger	H, M
Hendelses-varsling (Initiell)	Umiddelbar bekreftelse og eskalering av mottatte varsler fra leverandør.	Kontinuerlig (ved hendelse)	Vaktlag, IT/OT-drift	Hendelseslogg, varslingslogg	H, M
Fjerntilgangs-logger	Daglig/ukentlig gjennomgang av fjerntilgangslogger for OT/kritiske systemer.	Daglig (H), Ukentlig (M)	IT/OT-sikkerhet	Tilgangslogger, avvikslogg	H, M
Sårbarhet/ Patching	Oppfølging av leverandørens patchingstatus for OT-systemer.	Månedlig (H), Kvartalsvis (M)	IT/OT-sikkerhet	Patch-rapporter, sårbarhetsrapporter	H, M
Fysisk Sikkerhet OT	Periodisk sjekk av fysisk adgangskontroll til OT-utstyr/kontrollrom.	Ukentlig (H), Månedlig (M)	Produksjon/ Vedlikehold	Sjekklister, adgangslogger	H, M

Denne tabellen gir en oversikt over de mest detaljerte og hyppige kontrollene, som er viktige for daglig drift. Hvert punkt er direkte knyttet til en rutinemessig oppgave, slik at de kan følges opp av teamene som er ansvarlige for den daglige styringen.


BOUQUET
bama

Vedlegg E: Innhold til exitplan for kritiske og viktige IKT-leverandører

En exitplan er et strategisk dokument som beskriver prosessen for en kontrollert og strukturert avslutning av samarbeidet med en IKT-leverandør. Dette vedlegget er utarbeidet for å veilede virksomheter i matbransjen i utarbeidelsen av slike planer.

1.1. Hvorfor en exitplan?

En exitplan er viktig i god styring av leverandørrisiko. En slik plan skal sikre en kontrollert og strukturert avslutning av samarbeidet med en IKT-leverandør, uavhengig av om avslutningen er planlagt eller utløses av en krise.

Planen er en integrert del av virksomhetens overordnede planer for forretningskontinuitet og katastrofegjenoppretting, et krav som er eksplisitt nedfelt i NIS2 Artikkel 21(2)(c). NIS2-direktivet har som mål å etablere et «høyt felles cybersikkerhetsnivå» i samfunnskritiske sektorer. En god exitplan bidrar direkte til dette målet ved å bygge robusthet inn i leverandørkjeden, og dermed redusere sårbarheter som kan oppstå ved leverandørbytte eller -svikt.

For matbransjen er dette spesielt viktig, fordi en exitplan direkte støtter evnen til å sikre kontinuitet i matforsyningen og til å beskytte operasjonell stabilitet. En fraværende eller mangelfull exitplan for kritiske leverandører kan føre til alvorlige konsekvenser, inkludert betydelige operasjonelle forstyrrelser (som produksjonsstans eller -forstyrrelser) og manglende etterlevelse av NIS2 (med potensielle sanksjoner).

1.2. Hvilke leveranser og leverandører omfattes?

Exitplanen er spesifikt rettet mot kritiske og viktige IKT-leverandører. Kritikaliteten til en leverandørs tjeneste fastslås gjennom en konsekvensanalyse (BIA) og vurderingene som gjøres i «Vedlegg A: Veileder for vurdering av kritikaliteten på leveransen».

Fokuset på «kritikalitet» og «avhengighet» for leverandørkategorisering er grunnlaget for å prioritere innsatsen i exitplanleggingen. For eksempel vil en kritisk OT-leverandør med høy avhengighet (som en leverandør av et SCADA-system, som ofte er proprietært og vanskelig å erstatte) kreve den mest detaljerte, omfattende og proaktive exitplanleggingen. I kontrast kan en lavavhengig, ikke-kritisk IT-leverandør kun kreve en enklere, mer generell plan. Denne risikobaserte tilnærmingen sikrer at de mest betydelige truslene mot virksomhetens kjernevirksomhet blir adressert med passende grundighet.

2. Prinsipper for en robust exitplan

En effektiv exitplan er integrert med virksomhetens øvrige planer for forretningskontinuitet, og den tar høyde for å håndtere dynamiske risikoer.

2.1. Integrasjon med virksomhetens overordnede planer for forretningskontinuitet og katastrofegjenoppretting

Exitplanen er ikke et frittstående dokument, men en integrert del av virksomhetens overordnede plan for forretningskontinuitet (BCP) og katastrofegjenopprettingsplan (DRP).

Dette er et krav i NIS2 Artikkel 21(2)(c), som understreker den strategiske betydningen av en sømløs overgang. Denne integrasjonen sikrer at prosessene for å avslutte et leverandørforhold er i tråd med de overordnede strategiene for å opprettholde kritiske forretningsfunksjoner under forstyrrelser, enten det skyldes en planlagt avslutning eller en uforutsett hendelse. Videre bør ressurser, roller og kommunikasjonskanaler definert i BCP/DRP utnyttes og refereres til i exitplanen, slik at virksomheten har et sammenhengende rammeverk for kontinuitetsplanlegging.

2.2. Proaktiv planlegging og regelmessig revisjon

Exitstrategier bør ideelt sett utvikles ved kontraktsinngåelse eller tidlig i leverandørforholdet, spesielt for kritiske leverandører. Dette muliggjør bedre forhandling av exitklausuler, altså kontraktskrav som binder leverandøren til å utføre visse tjenester i transisjonsfasen der leveransen skal overtas av noen andre. Planen bør være et levende dokument som er gjenstand for regelmessig gjennomgang og oppdatering. Dette sikrer at planen er relevant i møte med endrede forretningsbehov, teknologiske fremskritt eller endringer i trusselbildet. Regelmessig testing av exitplanen, tilsvarende testing av BCP/DRP, er viktig for å verifisere at den er effektiv og for å identifisere eventuelle mangler eller svakheter før en reell situasjon oppstår.

2.3. Spesifikke hensyn for matbransjen

Exitplaner for matbransjen må inkludere de unike utfordringene knyttet til overføring av data, systemer og kompetanse relatert til komplekse og ofte proprietær operasjonell teknologi (OT)-systemer. Disse systemene er dypt integrert i fysiske prosesser, og planen må prioritere kontinuiteten i kritiske funksjoner. Avbrudd i disse funksjonene kan ha alvorlige konsekvenser for matsikkerhet og forsyningssikkerhet.

Muligheten for å ta driften internt («in-housing») kan være begrenset på kort sikt, spesielt for spesialiserte OT-systemer, Dette betyr at virksomheten må sørge for robuste alternative løsninger eller planlegge med lengre overgangsperioder.

3. Sentrale elementer i exitplanen

En exitplan må inkludere flere sentrale elementer for å sikre en kontrollert og effektiv overgang.

3.1. Triggere for iverksettelse av exitplanen

Planen må tydelig definere hendelser eller scenarier som kan utløse iverksettelsen av exitplanen. Disse triggerne kan være planlagte, f.eks. utløp av en kontrakt, en strategisk beslutning om leverandørbytte, innkjøp av tjenester internt, eller teknologisk foreldelse. De kan også være uplanlagte eller kriserelaterte, som at leverandøren går konkurs, et betydelig sikkerhetsbrudd hos leverandøren, vedvarende leveransefeil, manglende etterlevelse av NIS2-krav, force majeure-hendelser, eller omdømmetap for leverandøren.

For kritiske leverandører i matbransjen bør triggere knyttet til matsikkerhetshendelser, alvorlige forstyrrelser i forsyningskjeden, eller regulatorisk manglende etterlevelse (f.eks. gjentatte NIS2-brudd fra leverandørens side) inkluderes og overvåkes.

Definisjon av triggere, spesielt de som er knyttet til NIS2-etterlevelse og matbransjespesifikke risikoer, endrer exitplanen fra en ren beredskapsplan til en integrert del av proaktiv risikostyring og hendelseshåndtering. Ved å definere disse triggerne kan virksomheten reagere raskt når en situasjon oppstår. Dette er spesielt viktig for uplanlagte hendelser som sikkerhetsbrudd eller leverandørens finansielle ustabilitet, som direkte kan påvirke virksomhetens evne til å opprettholde drift. Tidlig oppdagelse av en trigger muliggjør en mer kontrollert og mindre reaktiv overgang. Dette innebærer at disse triggerne bør integreres i organisasjonens overordnede systemer for risikovervåking og hendelseshåndtering.

3.2. Roller, ansvar og organisering

Planen må definere tydelige roller og ansvar for alle interne interessenter som er involvert i exitprosessen. Dette kan inkludere prosjektledere, juridisk avdeling, innkjøpsavdeling, IT, OT, drift, kvalitetssikring, sikkerhet og kommunikasjon.

Styringsstrukturen, inkludert beslutningsmyndigheter, rapporteringslinjer og eskaleringsveier, må beskrives. En dedikert styringsgruppe kan være nødvendig for komplekse avslutninger. Det må spesifiseres hvordan den avtroppende leverandørens personell skal samhandle med det interne teamet og/eller den nye leverandøren under overgangen, inkludert tilgangsprotokoller og kommunikasjonskanaler. For matbransjen inkluderer dette gjerne spesialisert OT-personell (f.eks. kontrollteknikere, automasjonsspesialister, vedlikeholdsteknikere) og ledere for kvalitet/matsikkerhet.

3.3. Overføring og sikker sletting av data

Overføring og sikker sletting av data er et kritisk element i en exitplan.

3.3.1. Dataidentifikasjon og klassifisering

Alle datatyper som holdes eller behandles av den avtroppende leverandøren må identifiseres. Dette inkluderer både IT-data (f.eks. ERP-data, kundedata, finansielle poster) og OT-data (f.eks. SCADA-logger, sensordata, MES-produksjonsdata, batchposter, digitale sporbarhetsdata osv.). Datafølsomhet må klassifiseres (f.eks. personopplysninger, forretningshemmeligheter, kritiske operasjonelle data, immateriell eiendom) for å bestemme passende håndtering, sikkerhetstiltak og oppbevaringsperioder.

3.3.2. Overføringsmetoder og formater

Sikre metoder for dataoverføring må beskrives, som krypterte kanaler, sikre filoverføringsprotokoller, eller fysiske medier. Dataformater må spesifiseres for å sikre kompatibilitet med interne systemer eller den nye leverandørens plattformer. Dette er spesielt utfordrende for proprietære OT-dataformater, som kan kreve spesifikke konverteringsverktøy, mellomvare eller spesialisert ekspertise for å sikre brukbarhet og integritet etter overføringen.

3.3.3. Sikker sletting og bekreftelse

Prosedyrer for sikker og irreversibel sletting av alle virksomhetens data fra den avtroppende leverandørens systemer må beskrives. Dette inkluderer både primærlagring og sikkerhetskopier. Det skal kreves formell bekreftelse (f.eks. et destruksjonssertifikat eller en signert bekreftelse) fra leverandøren om at data er sikkert og irreversibelt slettet, i samsvar med kontraktsavtaler og relevante databeskyttelsesforskrifter (f.eks. GDPR, hvis personopplysninger er involvert).

Oversikt over data og overføringskrav

For en kompleks organisasjon kan det være nødvendig å utarbeide en tabell med en strukturert, detaljert og handlingsrettet oversikt over hvert spesifikke datasett.

Tabell 16. Eksempel på oversikt over datainventar ved overføring

Datakategori	Klassifisering	Volum	Format	Målformat
ERP-data	Kritisk	5 TB	SQL	SQL
SCADA-logger	Kritisk	20 TB	Proprietær binær	Proprietær binær/CSV
Kjølekjede-overvåking	Kritisk	1 TB	CSV/Proprietær	CSV
Sporbarhetsdata	Kritisk	3 TB	XML/Database	XML/Database
MES-produksjonsposter	Kritisk	10 TB	Proprietær database	Standardisert SQL
Kundedata	Sensitiv	500 GB	SQL	SQL
HR-data	Sensitiv	100 GB	Proprietær database	Standardisert SQL

En slik tabell inneholder et detaljert inventar, bidrar til å identifisere de unike egenskapene (klassifisering, format osv.), skisserer de spesifikke tekniske kravene for overføring og verifisering, og tildeler klare ansvarsområder. Tabellen kan derfor fungere som en operasjonell sjekkliste som gjør hele dataoverføringsprosessen reviderbar og verifiserbar.

Overføringsmetode	Integritetskontroll	Sletting bekreftelse	Ansvar (Int./ Ekst.)
Krypt. SFTP	Sjekksum	Attestasjon/Revisjonslogg	IT Drift, Ny leverandør
Fysisk disk/Dedikert VPN	Dataavstemming	Sertifikat av destruksjon	OT Engineering, avtroppende leverandør
API/Kryptert filoverføring	Stikkprøvekontroll	Attestasjon	Kvalitetssikring, IT-Drift
Sikker API/Direkte DB-dump	Dataavstemming	Attestasjon/Revisjonslogg	Produksjon, kvalitetssikring
Dedikert VPN/Dataekstraksjon	Sjekksum	Sertifikat av destruksjon	OT Engineering, Ny leverandør
Kryptert SFTP	Sjekksum	Attestasjon/Revisjonslogg	Juridisk, IT Drift
Kryptert SFTP	Sjekksum	Attestasjon/Revisjonslogg	HR, IT Drift

3.4. Overføring av systemer og teknisk infrastruktur

Denne delen omhandler den fysiske og logiske overleveringen av teknologiske eiendeler, inkludert både maskinvare og programvare.

3.4.1. Migrasjonsstrategier for IT-systemer

Strategi og plan for migrering av IT-systemer må defineres, f.eks. «lift-and-shift» til en ny skyleverandør, re-plattformering til en annen teknologistakk, eller re-faktorisering for intern hosting. Planen må inkludere hensyn til nettverkstilkobling, integrasjon med andre eksisterende interne systemer (f.eks. ERP og CRM), og avhengigheter av delte tjenester. Det må planlegges for parallelle operasjoner eller fasevise overganger for å minimere forstyrrelser i administrative og forretningsstøttefunksjoner.

3.4.2. Spesifikke utfordringer og løsninger for OT-systemer (SCADA, MES, etc.)

Overføring av komplekse og ofte proprietære OT-systemer som direkte kontrollerer og overvåker fysiske prosesser i en fabrikk kan medføre betydelige utfordringer. Disse systemene er typisk svært tilpassede og dypt integrerte i produksjonslinjene. Planen må håndtere proprietær maskinvare/programvare, spesialiserte industrielle grensesnitt (f.eks. PLS-er, sensorer) og sanntids prosesskontroll-logikk. Dette kan innebære spesialisert leverandørstøtte i migrasjonsfasen.

Overføringen av OT-systemer kan medføre økt risiko sammenlignet med IT-systemer. Dette kan kreve svært spesialisert planlegging, potensielt lengre tidslinjer og robuste beredskapstiltak for å sikre operasjonell drift. Proprietære OT-systemer innebærer ofte betydelig leverandørlåsning, begrenset interoperabilitet med andre systemer og avhengighet av høyt spesialiserte ferdigheter som ikke er lett tilgjengelige.

En slik lang planlegging, kan bety at en rask overgang ofte er umulig. Dette kan medføre komplekse fasevise migreringer, parallelle operasjoner, eller til og med manuelle tilbakefallsrutiner over lengre perioder. Dette innebærer at exitplanen for OT-leverandører må inkludere ekstraordinært detaljerte spesifikasjoner, leverandørspesifikke migreringsguider, og potensiell involvering av uavhengige spesialister innen OT-sikkerhet og automasjon.

Det betyr også at kontrakter med OT-leverandører ideelt sett bør inkludere klausuler som pålegger samarbeid under avslutning, gir tilgang til kritisk dokumentasjon. Virksomhetens BCP/DRP bør spesifikt modellere scenarier der OT-systemmigrering møter uventede forsinkelser eller feil.

3.4.3. Lisenser og immaterielle rettigheter

Eierskap og overførbarhet av alle relevante programvarelisenser, immaterielle rettigheter (IP) og proprietære konfigurasjoner relatert til tjenestene som avsluttes, må gjennomgås og avklares. Kontinuitet i lisensavtaler må sikres, eller nye avtaler med alternative leverandører må planlegges for å unngå juridiske problemer eller operasjonell stans. Dette er spesielt kritisk for spesialisert OT-programvare.

3.5. Overføring av kunnskap og kompetanse

Dette elementet sikrer at den nye enheten (enten et internt team eller en ny leverandør) effektivt kan administrere og drifte de overførte tjenestene og systemene.

3.5.1. Dokumentasjon av løsninger og prosesser

Den avtroppende leverandøren må pålegges å levere omfattende, oppdatert og forståelig dokumentasjon av alle systemer, konfigurasjoner, prosesser og operasjonelle prosedyrer. Dette inkluderer arkitekturdiagrammer, brukermanualer, feilsøkingsguider, sikkerhetskonfigurasjoner, og detaljert dokumentasjon for OT-systemer som kontroll-logikk, PLS-programmering og sensorkalibrering.

3.5.2. Opplæring og kompetanseoverføring til interne ressurser eller ny leverandør

Det må planlegges for strukturerte opplæringsøkter, workshops og praktisk gjennomgang for interne ansatte eller den nye leverandørens team. Nøkkelpersonell fra den avtroppende leverandøren som besitter kritisk kunnskap, må identifiseres, og deres tilgjengelighet under overgangsperioden for direkte kunnskapsoverføring må avtales. Fokus bør ligge på overføring av spesialisert OT-kunnskap, inkludert forståelse av industriell kontroll-logikk, spesifikke utstyrsfunksjonaliteter, feilsøking for produksjonskritiske systemer og sikkerhetsprotokoller.

3.5.3. Tilgang til teknisk ekspertise under overgangsperioden

Nivået og varigheten av støtte som kreves fra den avtroppende leverandøren etter oppsigelsesvarsel, spesielt for kritiske funksjoner, må defineres kontraktsmessig. Dette sikrer et sikkerhetsnett under den mest sårbare fasen. Dette kan inkludere tilstedeværelse på stedet, fjernstøtte eller et dedikert støtteteam for en definert periode for å sikre en jevn og stabil overlevering.

3.6. Identifisering og vurdering av alternative løsninger

Vurdering av alternative løsninger er en kjernekomponent for å sikre forretningskontinuitet.

3.6.1. Markedsanalyse og leverandørvalg

Det må utføres en grundig markedsanalyse for å identifisere mulige alternative IKT-leverandører som er i stand til å levere de nødvendige tjenestene. Omfattende due diligence (i henhold til Vedlegg B) må utføres på mulige nye leverandører, hvor deres kapasitet, finansielle stabilitet og samsvar med NIS2-krav og matbransjens spesifikke behov (f.eks. dokumentert OT-ekspertise og forståelse av matsikkerhetsforskrifter) vurderes.

3.6.2. Vurdering av «in-housing»

Muligheten for å ta tjenesten eller systemet internt («in-housing») må vurderes. Muligheten for «in-housing» kan være begrenset på kort sikt, spesielt for komplekse og spesialiserte OT-systemer. Slike systemer krever gjerne nødvendig infrastruktur, spesialiserte ferdigheter og betydelige investeringer. En kost-nytte-analyse som sammenligner intern drift med eksterne alternativer, må gjennomføres.

3.6.3. Kompatibilitet og integrasjonsutfordringer

Potensielle kompatibilitets- og integrasjonsutfordringer mellom nye løsninger og eksisterende interne systemer og prosesser må analyseres. Løsninger som minimerer forstyrrelser, sikrer sømløs integrasjon med kritiske produksjons- og forretningssystemer, og reduserer den totale angrepsflaten, bør prioriteres.

3.7. Tidslinje og milepæler for overgangen

En realistisk og grundig planlagt tidslinje er viktig for å sikre kontinuitet i kritiske funksjoner under overgangen.

3.7.1. Realistisk tidsplan for kritiske funksjoner

En detaljert og faseinndelt tidslinje som tar hensyn til kompleksiteten i overgangen, må utvikles. Uavbrutt drift av kritiske funksjoner må prioriteres, med mål om null nedetid der det er mulig. Bufferperioder for uforutsette forsinkelser, tekniske utfordringer eller personellproblemer må inkluderes.

3.7.2. Overgangsfaser (planlegging, testing, implementering og stabilisering)

Overgangen bør brytes ned i håndterbare faser, med klare mål, leveranser og suksesskriterier for hver fase. Testfasen må vektlegges for å validere funksjonalitet, sikkerhet og ytelse før full overgang. Dette inkluderer integrasjonstesting, brukerakseptansetesting, sikkerhetstesting og ytelsestesting.

Eksempel på tidslinje og milepæler for en kritisk OT-leveranse

Tabell 17. Eksempel på faseinndelt tidslinje

Fase	Nøkkelmilepæler	Varighet	Avhengigheter	Ansvarlig	Kritikalitet
Planlegging og leverandørvalg	Kontrakt signert med ny leverandør	8 uker	Intern ressursallokering, markedsanalyse	Prosjektleder, Innkjøp	Lav
Datamigrering	Datatransfer fullført	6 uker	Avtroppende leverandørsamarbeid, IT/OT Team	IT Drift, OT Engineering	Medium
Nytt system bygging og konfigurasjon	Nytt SCADA-system installert, grunnkonfigurasjon	12 uker	Maskinvareleveranse, ny leverandør	Ny leverandør, OT Team	Medium
Integrasjonstesting	Integrasjonstester bestått, OT-nettverks-segmentering verifisert	4 uker	Intern IT/OT, ny leverandør, avtroppende leverandør	IT/OT Sikkerhet	Medium
Brukerakseptanse-testing (UAT)	UAT godkjent av produksjon	3 uker	Produksjonsteam, Kvalitetssikring	Produksjon, Kvalitetssikring	Lav
Parallell drift	Stabil drift med begge systemer	2 uker	Produksjonsteam, IT/OT Drift	Produksjon, IT/OT Drift	Høy
Overgang	Produksjon «go-live» på nytt system	1 dag (planlagt nedetid)	Alle team	Prosjektleder	Høy (kritisk)
Stabilisering og avvikling	Gammelt system avviklet	4 uker	IT/OT Drift	IT/OT Drift	Lav

Tabellen hjelper med å identifisere potensielle flaskehalser og ressurskonflikter Den bidrar til proaktiv risikoidentifikasjon (f.eks. hvis en avhengighet blir forsinket) og er et godt grunnlag for oppfølging fra prosjektledere, toppledelse og alle involverte interessenter. Den fungerer også som et godt kommunikasjonsverktøy, som sikrer at alle parter forstår sekvensen og timingen av hendelser. Slik kan den bidra til å minimere operasjonell risiko og potensielle problemer under en svært sensitiv overgang.

3.8. Kommunikasjonsplan

En kommunikasjonsplan for alle interne og eksterne interessenter bør utvikles.

3.8.1. Intern og ekstern kommunikasjon

Kommunikasjonskanaler, frekvens og budskap for ansatte, kunder, leverandører (både avtroppende og nye), partnere og relevante reguleringsorganer (f.eks. Mattilsynet eller Nasjonal sikkerhetsmyndighet) må defineres. Åpenhet må sikres samtidig som sensitiv informasjon beskyttes.

3.8.2. Håndtering av omdømmerisiko

Potensielle omdømmerisikoer knyttet til et leverandørbytte, tjenesteforstyrrelse eller krise-drevet avslutning må adresseres. Strategier for proaktiv og konsekvent kommunikasjon må utvikles for å opprettholde tilliten hos kunder, publikum og bransjens interessenter.

3.9. Risikostyring under overgangen

Selve avslutningsprosessen introduserer nye risikoer som må håndteres.

3.9.1. Identifisering av risikoer og sårbarheter

En spesifikk risikovurdering for overgangsperioden må gjennomføres for å identifisere potensielle forstyrrelser, nye sårbarheter og operasjonelle utfordringer. Risikoer knyttet til leverandørens manglende samarbeid, tekniske inkompatibiliteter, kompetansegap i det nye teamet og potensial for datatap eller -korrupsjon må vurderes.

3.9.2. Avbøtende tiltak og beredskapsplaner

Spesifikke avbøtende tiltak for alle identifiserte risikoer må defineres, inkludert beredskapsplaner og tilbakefallsrutiner for kritiske funksjoner. Den overordnede BCP/DRP må integreres i arbeidet med exitplanen.

3.10. Testing og validering

Testing og validering er nødvendig for å sikre en jevn, sikker og funksjonell overgang.

3.10.1. Testplan for overførte systemer og data

En detaljert testplan som dekker funksjonell testing, ytelsestesting, sikkerhetstesting og integrasjonstesting av alle overførte systemer og data i det nye miljøet, må utvikles. Spesifikke testtilfeller for OT-systemer må inkluderes.

3.10.2. Verifisering av funksjonalitet og sikkerhet

Grundig validering må utføres for å sikre at alle kritiske funksjoner fungerer som forventet, oppfyller ytelseskrav, og at sikkerhetskontroller (f.eks. tilgangskontroller, kryptering, nettverkssegmentering) er korrekt implementert og effektive i det nye miljøet.

3.11. Formell avslutning og etterarbeid

De siste trinnene for å formelt avslutte forholdet og sikre kontinuerlig forbedring.

3.11.1. Kontraktsmessig avslutning

Alle kontraktsforpliktelser må sikres oppfylt av begge parter, inkludert sluttbetalinger, retur av virksomhetens eiendeler og formelle oppsigelsesvarsler. Det må verifiseres at alle klausuler knyttet til datasletting, overføring av immateriell eiendom og støtte etter opphør er fullt ut oppfylt og dokumentert.

3.11.2. Sluttrapportering og evaluering

En sluttrapport om exitprosessen bør utarbeides. Denne bør dokumentere nøkkelaktiviteter, suksesser, utfordringer, læringspunkter og forbedringsområder. En etteranalyse med alle sentrale interessenter bør gjennomføres for å forbedre fremtidige exitplaner og virksomhetens leverandørstyring, slik at erfaringene kan bidra til organisatorisk læring.

4. Vedlikehold og revisjon av exitplanen

Exitplanen er et dynamisk dokument som krever regelmessig vedlikehold og revisjon. Planen bør gjennomgås og oppdateres minst årlig, eller når det er betydelige endringer i leverandørforholdet, interne systemer, forretningsprosesser eller relevante regulatoriske krav (f.eks. oppdateringer til NIS2 eller relaterte lover).

Regelmessige øvelser og simuleringer av exitplanen, spesielt for kritiske OT-leverandører, kan være viktig for å sikre at den er praktisk gjennomførbar. Disse øvelsene bidrar til å identifisere mangler og forbedre prosedyrer.

En slik proaktiv tilnærming reduserer risikoen for at en «papirplan» mislykkes i et reelt scenario, og forsterker dermed den generelle robustheten og motstandskraften i matforsyningskjeden mot digitale og operasjonelle forstyrrelser. Den støtter også direkte NIS2-prinsippet om kontinuerlig risikostyring og tilpasning for å opprettholde et høyt nivå av cybersikkerhet.

Vedlegg F: Sjekkliste for exitplan

Denne sjekklisten er et verktøy for å verifisere at en exitplan for en kritisk eller viktig IKT-leverandør er komplett og robust. Den skal brukes for å sikre at alle nødvendige vurderinger, prosesser og ansvarsområder beskrevet i «Vedlegg E: Innhold til exitplan» er dekket. Sjekklisten skal hjelpe virksomheten med å systematisk validere planen for å sikre en kontrollert avslutning av leverandør-forholdet, minimere operasjonell risiko og ivareta kravene i NIS2.

Sjekklisten kan også brukes i de periodiske gjennomgangene av exitplanen.

1. Veiledning til sjekklisten

Gå gjennom hvert sjekkpunkt og marker status. Bruk kommentarfeltet til å utdype, referere til spesifikke deler av exitplanen, eller notere avvik og nødvendige tiltak.

Status:

- OK: Kravet er tilfredsstillende dekket i exitplanen.
- Avvik: Kravet er mangelfullt eller ikke dekket. Tiltak må iverksettes.
- I/A: Ikke aktuelt for denne spesifikke leverandøren/tjenesten. Begrunnelse bør gis i kommentarfeltet.

Leverandør: [Fyll inn navn på IKT-leverandør]
Tjeneste: [Beskriv den kritiske/viktige tjenesten]
Dato for gjennomgang: [Fyll inn dato]
Ansvarlig for gjennomgang: [Fyll inn navn/rolle]

Tabell 18. Sjekkliste for exitplan

Nr.	Sjekkpunkt	Status (OK, Avvik, I/A)	Kommentarer / Referanse i plan / Tiltak
1.0	Generelt og forankring		
1.1	Er exitplanen tydelig merket med leverandør, tjeneste, versjonsnummer og dato?		
1.2	Er eier av exitplanen (rolle/person) tydelig definert?		
1.3	Er planen formelt godkjent av ledelsen?		
1.4	Er det definert en prosess for årlig (eller hendelsesstyrt) gjennomgang og revisjon av planen?		
2.0	Triggere for iverksettelse		
2.1	Er både planlagte (f.eks. kontraktutløp) og uplanlagte (f.eks. konkurs eller vesentlig mislighold) triggere definert?		
2.2	Er triggere spesifikt knyttet til NIS2-brudd (f.eks. manglende rapportering ved hendelser eller gjentatte sikkerhetsavvik) inkludert?		
2.3	Er triggere spesifikt knyttet til matsikkerhet eller forsyningssikkerhet definert?		
2.4	Er prosessen for å formelt beslutte og kommunisere iverksettelse av planen beskrevet?		
3.0	Roller, ansvar og organisering		
3.1	Er et dedikert exit-team med definerte roller og ansvar (inkl. IT, OT, juridisk, sikkerhet, kvalitet og innkjøp) etablert?		
3.2	Er en overordnet styringsstruktur (f.eks. styringsgruppe) med beslutningsmyndighet og eskaleringsveier beskrevet?		

3.3	Er den avtroppende leverandørens forventede roller og ansvar under overgangen definert (og kontraktsfestet)?
4.0	Dataoverføring og sikker sletting
4.1	Er alle data som behandles av leverandøren identifisert, klassifisert og dokumentert?
4.2	Er tekniske metoder og formater for dataoverføring spesifisert for å sikre kompatibilitet?
4.3	Er det etablert prosedyrer for å verifisere dataintegritet og fullstendighet etter overføring?
4.4	Er det en prosedyre for sikker og verifiserbar sletting av virksomhetens data fra alle leverandørens systemer (inkl. backuper)?
4.5	Er det krav om et destruksjonssertifikat eller tilsvarende bekreftelse fra leverandøren?
5.0	Overføring av systemer og infrastruktur
5.1	Er det utarbeidet en komplett oversikt over all relevant maskinvare, programvare og lisenser?
5.2	Er migrasjonsstrategi for IT-systemer definert?
5.3	Er det en spesifikk og detaljert plan for overføring av OT-systemer, inkludert håndtering av proprietær teknologi og minimering av produksjonsstans?
5.4	Er eierskap og overførbarhet av lisenser og immaterielle rettigheter (IP) avklart?
6.0	Kunnskapsoverføring og kompetanse
6.1	Er det stilt krav til levering av komplett og oppdatert teknisk og operasjonell dokumentasjon?
6.2	Er det en plan for opplæring og kompetanseoverføring til internt personell eller ny leverandør, med særlig fokus på spesialisert OT-kunnskap?
6.3	Er tilgang til nøkkelpersonell hos avtroppende leverandør i en overgangsperiode sikret (kontraktsmessig)?
7.0	Alternative løsninger
7.1	Er mulige alternative leverandører identifisert og vurdert (due diligence)?
7.2	Er muligheten for å ta tjenesten internt («in-housing») analysert?
7.3	Er kompatibilitet og integrasjonsutfordringer med en ny løsning kartlagt?
8.0	Tidslinje og milepæler
8.1	Er det utarbeidet en detaljert og realistisk tidslinje med faser, aktiviteter og tydelige milepæler?

8.2	Tar tidslinjen spesielt hensyn til kontinuitet i kritiske funksjoner?
8.3	Er kritiske avhengigheter mellom aktiviteter identifisert?
8.4	Er det allokert et eget budsjett for gjennomføring av exit-prosessen?
9.0	Kommunikasjonsplan
9.1	Er det definert en plan for kommunikasjon til alle relevante interne og eksterne interessenter?
9.2	Er strategier for å håndtere omdømmerisiko, spesielt ved en krise-drevet exit, beskrevet?
10.0	Risikostyring under overgangen
10.1	Er det gjennomført en spesifikk risikovurdering for selve overgangsperioden?
10.2	Er avbøtende tiltak og beredskapsplaner for de identifiserte risikoene definert?
10.3	Er det etablert tekniske og operasjonelle tilbakefallsrutiner («rollback plans») for kritiske steg i overgangen?
11.0	Testing og validering
11.1	Er det en detaljert testplan som dekker funksjonalitet, integrasjon, ytelse og sikkerhet for den nye løsningen?
11.2	Er det definert klare og målbare suksesskriterier for testingen?
11.3	Er det planlagt for brukerakseptansetest (UAT) med personell fra drift/produksjon?
12.0	Formell avslutning og evaluering
12.1	Er det en prosedyre for å verifisere at alle kontraktsmessige forpliktelser er oppfylt før endelig avslutning?
12.2	Er prosessen for formell signering og godkjenning av en fullført overgang beskrevet?
12.3	Er det planlagt en evalueringsprosess («lessons learned») for å fange opp erfaringer til forbedring av fremtidige exitplaner?

Vedlegg G: Triggere for iverksettelse av exitplan

Dette vedlegget inneholder en liste med eksempler på hendelser og scenarioer (triggere) som bør eller kan utløse en gjennomgang eller iverksettelse av en exitplan for en kritisk eller viktig IKT-leverandør. Formålet er å etablere et system for å identifisere risikosignaler på et tidlig stadium, slik at virksomheten kan være proaktiv fremfor reaktiv.

Listen er ikke uttømmende, og virksomheten må selv vurdere hvilke triggere som er mest relevante for sine leverandørforhold. Disse triggerne bør integreres i den kontinuerlige overvåkingen av leverandører (beskrevet i veilederens kapittel 4.4). En utløst trigger betyr ikke nødvendigvis en umiddelbar avslutning, men skal alltid føre til en formalisert vurdering.

Handlingen som følger en utløst trigger, bør være proporsjonal med risikoen:

- **Gjennomgang av exitplan**
  Utløses ved tidlige varselsignaler eller mindre alvorlige hendelser. Formålet er å verifisere at eksisterende plan er oppdatert, relevant og dekkende for det aktuelle scenarioet.

- **Iverksettelse av exitplan**
  Utløses ved alvorlige, bekreftede hendelser som utgjør en uakseptabel risiko for virksomhetens drift, sikkerhet eller omdømme.

1. Operasjonelle og ytelsesrelaterte triggere

Disse triggerne er knyttet til leverandørens evne til å levere avtalt tjenestekvalitet og ytelse.

Tabell 19. Eksempel på operasjonelle og ytelsesrelaterte triggere

Nr.	Trigger	Beskrivelse
1.1	Vedvarende tjenesteavbrudd	Gjentatte eller langvarige avbrudd i tjenesten som påvirker kritiske forretningsprosesser, som produksjonskontroll (OT), kjølekjedestyring eller sporbarhetssystemer.
1.2	Vesentlig brudd på servicenivåavtaler (SLA)	Gjentatt eller alvorlig svikt i å møte definerte mål for oppetid, responstid, feilretting eller support.
1.3	Forringet tjenestekvalitet	En merkbar og vedvarende nedgang i kvaliteten på leveransen som påvirker matsikkerhet, produktkvalitet, dataintegritet eller brukeropplevelse.
1.4	Manglende evne til feilretting	Leverandøren viser manglende evne eller vilje til å identifisere rotårsak og implementere varige løsninger på gjentakende problemer.
1.5	Utilfredsstillende support	Vedvarende dårlig tilgjengelighet, kompetanse eller serviceinnstilling fra leverandørens supportorganisasjon.

2. Sikkerhetsrelaterte triggere

Disse triggerne er direkte knyttet til cybersikkerhet og leverandørens evne til å beskytte informasjon og systemer i henhold til NIS2-kravene.

Tabell 20. Eksempel på sikkerhetsrelaterte triggere

Nr.	Trigger	Beskrivelse
2.1	Betydelig sikkerhetshendelse	Leverandøren opplever et datainnbrudd, løsepengevirusangrep eller en annen alvorlig sikkerhetshendelse som påvirker eller kan påvirke virksomhetens data eller tjenester.
2.2	Brudd på varslingsplikt (ref. NIS2 Art. 23)	Leverandøren unnlater å varsle virksomheten om en sikkerhetshendelse innenfor den kontraktsfestede tidsfristen, noe som setter virksomhetens egen rapporteringsplikt til myndighetene i fare.
2.3	Alvorlige funn i sikkerhetsrevisjoner	Identifisering av kritiske eller høye sårbarheter eller avvik i uavhengige revisjoner (f.eks. SOC 2, ISAE 3402), penetrasjonstester eller egne vurderinger, som leverandøren ikke håndterer tilfredsstillende.
2.4	Manglende etterlevelse av grunnleggende sikkerhetstiltak	Dokumentert svikt i etterlevelse av avtalte sikkerhetskrav som sårbarhetshåndtering (patching), sikker fjerntilgang (MFA), nettverkssegmentering eller fysisk sikring av OT-utstyr.
2.5	Svikt i leverandørkjedesikkerhet	Leverandøren kan ikke dokumentere tilstrekkelig kontroll på sine egne kritiske underleverandører, eller en hendelse hos en underleverandør rammer tjenesten.
2.6	Uautorisert aktivitet	Oppdagelse av uautorisert tilgang til, endring eller eksfiltrering av virksomhetens data.

3. Kontraktsmessige og kommersielle triggere

Disse triggerne omhandler det forretningsmessige og juridiske grunnlaget for samarbeidet.

Tabell 21. Eksempel på kontraktsmessige og kommersielle triggere

Nr.	Trigger	Beskrivelse
3.1	Planlagt utløp av kontrakt	Kontrakten nærmer seg utløpsdato uten at det er enighet om eller intensjon om fornyelse.
3.2	Vesentlig mislighold	Leverandøren bryter sentrale forpliktelser i avtalen på en måte som gir rett til heving.
3.3	Leverandørens finansielle ustabilitet	Leverandøren går konkurs, er under gjeldsforhandling, eller det foreligger andre klare tegn på finansiell ustabilitet som truer den langsiktige leveranseevnen.
3.4	Uakseptable kontraktsendringer	Leverandøren fremtvinger urimelige endringer i priser eller vilkår som ikke er i tråd med avtalen.

4. Strategiske og organisatoriske triggere

Disse triggerne er knyttet til endringer hos leverandøren eller i markedet som påvirker det strategiske samarbeidet.

Tabell 22. Eksempel på strategiske og organisatoriske triggere

Nr.	Trigger	Beskrivelse
4.1	Oppkjøp eller fusjon	Leverandøren blir kjøpt opp av eller fusjonerer med en annen aktør, spesielt en konkurrent eller et selskap med en annen strategisk retning, risikoprofil eller lavere sikkerhetsstandard.
4.2	Endring i strategisk fokus	Leverandøren endrer sin forretningsstrategi eller produktportefølje slik at tjenesten som leveres til virksomheten ikke lenger er et kjerneområde, blir avviklet («end-of-life») eller ikke videreutvikles.
4.3	Tap av nøkkelpersonell	Kritisk kompetanse forsvinner hos leverandøren uten at den blir tilfredsstillende erstattet.
4.4	Alvorlig omdømmetap	Leverandøren involveres i negativ medieomtale, skandaler eller etiske overtramp som kan skade virksomhetens eget omdømme.
4.5	Endring i egen strategi	Virksomhetens egen strategiske beslutning om å bytte teknologiplattform, konsolidere leverandører, eller ta tjenesten internt («in-housing»).

5. Force majeure og regulatoriske triggere

Disse triggerne omhandler ytre hendelser utenfor partenes kontroll.

Tabell 23 Eksempler på force majeure og regulatoriske triggere

Nr.	Trigger	Beskrivelse
5.1	Langvarig force majeure	En force majeure-hendelse (naturkatastrofe, pandemi, krig etc.) fører til at leverandøren ikke kan levere tjenesten over en lengre periode, og det er usikkerhet rundt gjenopptakelse.
5.2	Endrede regulatoriske krav	Nye lover eller forskrifter trer i kraft som leverandøren ikke kan eller vil etterleve, og som er nødvendige for virksomhetens drift eller etterlevelse.

Næringslivets
sikkerhets-
råd

www.nsr-org.no