NIS2-koncepter til
kommunal implementering

Forsyningskædesikkerhed

KL

Forord

Som del af den fælleskommunale digitale handlingsplan 2021-2025 har KL i samarbejde med en række kommuner og med ekstern konsulentbistand igangsat projekt til støtte for kommunernes arbejde med cybersikkerhed, specifikt ift. implementering af NIS2. Leverancen herfra er en kommunale NIS2-drejebog. Dette dokument er et kapitel til denne drejebog.

Den fælleskommunal NIS2-drejebog har til formål at understøtte og inspirere kommunernes arbejde med egen cybersikkerhed. Dette gøres via redskaber, skabeloner, årshjul, eksempler mv. der indgår i drejebogen. 16 kommuner har i fire temagrupper bidraget med egen erfaring og input, således at materialet afspejler kommunale behov og vilkår, baseret på kommunal erfaring, baseret på kommunal erfaring.

Drejebogen indeholder bud på, hvordan man som kommune kan arbejde med fire centrale NIS2-temaer: Risikovurdering, Ledelsesansvar, Forsyningskædesikkerhed og Hændelseshåndtering.

De to første Drejebogskapitler (Ledelsesansvar og Risikovurdering) publiceres i december 2025 og kan frit bruges. De to følgende drejebogskapitler forventes publiceret i løbet af februar 2026, hvor materialet for alle fire kapitler udgives i én samlet kommunal NIS2-drejebog.

Drejebogen giver anbefalinger til oversættelse og operationalisering - men ikke gengivelse - af NIS2-krav. I materialet synliggøres desuden de konkrete krav og forpligtelser fra NIS2-loven og vejledninger, således at man som kommune kan se sammenhæng hertil.

Materialet er udarbejdet med blik for, at såvel store som mindre kommuner skal kunne se sig selv i det. Samtidigt er der taget højde for øvrige forskelle kommunerne imellem. I sidste ende skal kommunen selv tage stilling og kunne begrunde egne valg bl.a. ifm. et tilsyn.

Udgangspunktet er, at ansvaret for NIS2-efterlevelse og sikkerhedsniveau ligger hos kommunen selv. Topledelsens (direktionen) ansvar er helt centralt for at få arbejdet med cybersikkerhed forankret og prioriteret i kommunen.

Opgaver kan dog uddelegeres. Det er således vigtigt at forholde sig til, hvordan og hvilke beslutninger der træffes hvor og hvor ofte.

Drejebogstema Forsyningskædesikkerhed
I dette kapitel af den kommunale NIS2-drejebog præsenteres en tilgang til kommunens håndtering af forsyningskædesikkerhed, hvorved kommunen kan få inspiration og støtte til at få overblik over leverandører og it-understøttelsen af kommunens opgaver.

Drejebogsmaterialet giver redskaber til at foretage en screening af leverandørerne og bidrager med overblik over kommunens anskaffelser, fra processen initieres til aftalen slutter. Der gives desuden input til, hvordan man stiller de rette krav til leverandøren og produkterne. Altsammen således at kommunerne kan opretholde en tilstrækkelig og passende forsyningskædesikkerhed.

Forsyningskædesikkerhed er et af de bærende elementer i NIS2-implementering og adresserer sårbarheder og afhængigheder ift. de leverandører og IT-produkter man baserer sin opgavevaretagelse på. NIS2 sætter fokus på at kende sin it-portefølje og være bevidst om, hvor eventuelle svagheder er eller kan opstå og dermed være godt klædt på til at stille passende krav til leverandøren.

Tanken i NIS2-sammenhæng er, at sårbarheder i forsyningskæden kan føre til alvorlige konsekvenser for kommunens drift. Dertil er det vigtigt at være bevidst om sammenhænge på tværs af sin IT-portefølje, da en sårbarhed et sted, kan føre til kompromittering eller nedbrud et andet. Det kræver en systematik og overblik at håndtere dette. NIS2-drejebogen giver en fælles metode, man kan vælge at bruge (helt eller delvist).

Desuden har man som kommune stor hjælp at hente i de fælleskommunale samarbejder som fx Det Fælleskommunale Databehandlersekretariat, KOMBIT/KommuneCert samt SKI. Disse aktører kan hjælpe kommunerne med at løfte i flok, så kravene bliver mere håndtérbare, såvel for kommuner som for de leverandører, som kommunerne indgår aftaler med.

Kommunerne kan have eksisterende processer og metoder for leverandøroverblik og kravstillelse. Det fælles materiale i NIS2-drejebogen kan her give anledning til at se, om der er behov for at justere eller blot sikre sig, at man kan forklare og begrunde at man har et tilstrækkeligt niveau i tilfælde af NIS2-tilsyn og for at man er rustet til de løbende beslutninger ifm. anskaffelser.

Som enhed er det ens ansvar at sikre sig, at ens IT-leverandører ift. kritikalitet i NIS2 vedligeholder et sikkerhedsniveau, der tilsvarer ens kommunes risikovurdering af den pågældende opgave.

Drejebogsmateriale giver således metode til, hvordan man som kommune kan gå til værks. Materialet omfatter desuden inspiration fra kommuner, der kan bruges i egne lokale overvejelser.

Baggrund
Den danske NIS2-lov trådte i kraft 1. juli 2025 med det formål at højne og ensartet cybersikkerheden – på tværs af EU og på tværs af sektorer i EU-medlemslandene. NIS2-loven udmønter EU's Netog Informationssikkerhedsdirektiv (NIS2).

Fokus i NIS2 er at opretholde driftskontinuitet og sikre robustheden over for cyberangreb på samfundskritiske områder. NIS2 har fokus på at forhindre hændelser og udlevelsen af konsekvenserne af angreb Det stiller krav til, at man som omfattet enhed har overblik over sammenhænge mellem kommunale arbejdsprocesser og IT-systemer at kunne vurdere konsekvenser ved hændelser og være i stand til at håndtere og indrapportere kritiske hændelser. Man skal også som omfattet enhed være opmærksom på kritiske led i ens forsyningskæder og leverandører.

Kommunerne er omfattet som helhed, dvs. alle IT-systemer og opgaver pga. kommunernes tværgående opgaver og nære kontakt til borgerne på vitale områder. Ved eksempelvis sundhedsområdet, gør at kommunerne i NIS2 udpeges som væsentlig enhed.

Styrelsen for Samfundssikkerhed (SAMSIK), der er overordnet NIS2-ansvarlig myndighed i Danmark, har lanceret fire generelle vejledninger og en Kommunevejledning: NIS 2-vejledninger | Styrelsen for Samfundssikkerhed

Vejledninger og selve NIS2-loven danner udgangspunkt for arbejdet med den kommunale NIS2-drejebog og de koncepter for implementering, der her gives. SAMSIK har desuden lanceret infosiden 'Introduktion til Risikovurdering' på Sikker Digital. Her har SAMSIK samlet viden og gode råd om digital sikkerhed: Introduktion til risikostyring. Sikker Digital og materialet kan være godt at orientere sig i for mange, bl.a. ift. NIS2 men også risikovurderinger i øvrigt.

Den kommunale NIS2-drejebog og redskaber adresserer tilsvarende emner, men tilpasset en kommunal kontekst. Det samme gælder for det sikkerheds-relaterede materiale på KL's Videnscenter, der kan være et godt sted at starte for mange kommuner: Cyber- og informationssikkerhed.

Indholdsfortegnelse

Indhold

Bilag

3.1 Forsyningskædesikkerhed under NIS2

Arbejdet med forsyningskædesikkerhed skal tage afsæt i at kommunerne – som *væsentlige enheder* defineret i § 4 i NIS2-loven – er forpligtet til at etablere og anvende procedurer for leverandørstyring, der sikrer både forsyningssikkerhed og cybersikkerhed i samarbejdet med direkte leverandører og tjenesteudbydere, i det omfang deres ydelser kan påvirke sikkerheden i relation til de tjenester, der gør enheden omfattet af NIS2, jf. § 6, stk. 4 i NIS2-loven.

I overensstemmelse med vejledning til NIS2-loven om implementering af cybersikkerhedsforanstaltninger, afsnit 4 "Forsyningskædesikkerhed" gælder det, at enheden SKAL implementere procedurer for leverandørstyring, som:

- sikrer både forsyningssikkerhed og cybersikkerhed i samarbejdet med direkte leverandører og tjenesteudbydere, og understøtter en systematisk identifikation og vurdering af risici forbundet med specifikke leverandører og deres ydelser
  og
- muliggør indgåelse og håndhævelse af aftaler, der dokumenterer leverandørens overholdelse af krav til forsynings- og cybersikkerhed, herunder krav om relevante sikkerheds-foranstaltninger, rapportering, hændelses-håndtering samt mulighed for tilsyn og kontrol.

Disse krav indebærer, at leverandørstyring ikke alene handler om kontraktuelle forhold, men udgør en kontinuerlig, risikobaseret proces, der skal understøtte kommunens samlede sikkerhedsniveau og sikre en vedvarende, dokumenteret og effektiv håndtering af risici i hele leverandørforholdets livscyklus.

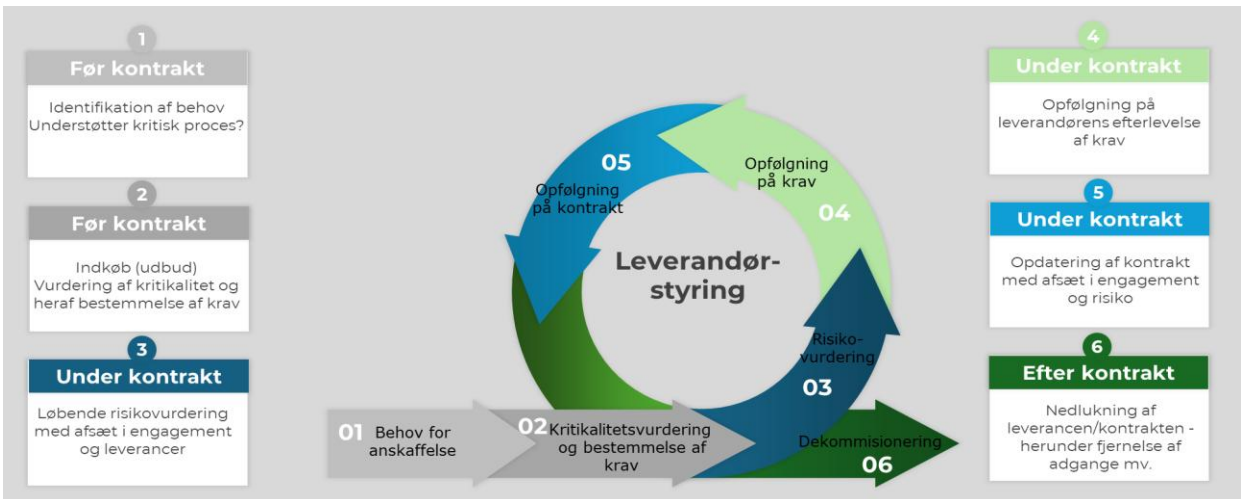
Dette er operationaliseret gennem en leverandørcyklus - Model 3.2.1, som strukturerer leveranceforløbet – fra behovsafdækning og leverandørvalg, gennem kontraktindgåelse og løbende opfølgning, til udfasning og afslutning af samarbejdet.

Model 3.2.1 og drejebogen tager afsæt i vejledning til NIS2 loven "Implementering af cybersikkerhedsforanstaltninger" og fungerer som et praktisk værktøj, der understøtter en ensartet, dokumenteret og risikobaseret tilgang til kommunens håndtering af eksterne leverandører og tjenesteudbydere.
Formålet er at sikre, at kommunen opretholder et højt og konsistent sikkerhedsniveau – både internt og i hele den forsyningskæde, der understøtter kommunens opgavevaretagelse.

Det er op til den enkelte kommune at beslutte, i hvilket omfang faserne i leverandørcyklussen skal indgå i deres "Disposition til procedure for levenandørstyring" samt hvordan vurderinger og krav til nye leverandører f.eks. kan indarbejdes i kommunens eksisterende procedurer for indkøb.

I det følgende gennemgås de enkelte faser i leverandørcyklusmodellen. Det er vigtigt at skelne mellem eksisterende løsninger/tjenesteydelser eller nye, da modellens faser, finder anvendelse på forskellige tidspunkter.

3.2 Leverandørcyklus



Model3.2.1

Før kontrakt – Fase 1–2

Denne del af processen omfatter alle aktiviteter fra behovsafdækning til indgåelse af kontrakt. Formålet er at sikre, at kommunen foretager et oplyst, risikobaseret og sikkerhedsbevidst valg af leverandør, og at de nødvendige sikkerhedskrav er tydeligt fastlagt før samarbejdet påbegyndes. Fase 1-2 finder anvendelse ved anskaffelse af nye løsninger eller tjenesteydelser.

1.1 Behovsafdækning og vurdering af proces

Kommunen identificerer et behov for enten en ny IT-løsning eller tjenesteydelse. Når kommunen skal sikre et passende sikkerhedsniveau vurderes det om IT-løsningen eller tjenesteydelsen understøtter en kritisk proces som defineret i drejebogens kapitel om Risikostyring, specifikt afsnit 2.4 "Identifikation af kritiske processer, systemer og tjenester".

2.1 Kritikalitets- og risikovurdering af leverance

I henhold til Vejledning til NIS2-loven "Implementering af cybersikkerhedsforanstaltninger" afsnit 4 - Forsyningskædesikkerhed bør kommunen anvende en risikobaseret tilgang, så kravene til den enkelte leverandør eller tjeneste-udbyder fastsættes proportionalt med leverancens betydning for kommunens forsynings- og cybersikkerhed, og unødigt høje krav dermed undgås.
For at kunne stille krav til leverandøren på baggrund af en risikobaseret tilgang gennemføres en kritikalitetsvurdering jf. "Guide til identifikation af kritiske leverandører" fase 3-6.
På baggrund af vurderingen fastlægges de overordnede sikkerhedskrav. Kravene differentieres efter kritikalitetsniveau (fx K1–K4 i henhold til SKI's scoringsmodel).
Hvis anskaffelsen ift. NIS2 sker via SKI eller gennem en KOMBIT-anskaffelse vil mange krav typisk allerede være indarbejdet i den gældende kontrakt.
Kritikalitets- og risikovurdering dokumenteres og godkendes af relevante roller – typisk systemejer og IT-sikkerhed.

2.2 Udbud/indkøb og leverandørvalg

Udbudsmateriale og kravspecifikation udformes på baggrund af de identificerede sikkerhedsbehov. Dette indebærer bl.a.:

- Krav til sikkerhedsstandarder (fx ISO 27001 eller tilsvarende)
- Krav om hændelsesrapportering og underretningsfrister
- Auditret og dokumentationskrav
- Krav til adgangsstyring, dataopbevaring, databehandlere mv.
- Evalueringskriterier for leverandørens sikkerhedspraksis

Formålet er at sikre, at sikkerhed er en integreret del af alle anskaffelser – og ikke et efterfølgende tillæg.

2.3 Leverandørscreening

I henhold til Vejledning til NIS2-loven "Implementering af cybersikkerhedsforanstaltninger" afsnit 4 - Forsyningskædesikkerhed bør kommunen definere kriterier for, hvordan de udvælger leverandører eller tjenesteudbydere.
For den foreløbigt valgte leverandør gennemføres en screening, der vurderer leverandørens:

- Organisatoriske og tekniske kapabiliteter
- Efterlevelse af sikkerhedsstandarder
- Historik vedrørende drift, sikkerhed og compliance
- Evne til at understøtte kommunens behov og kontraktuelle krav

Screeningen reducerer risikoen for at vælge en leverandør, der ikke kan leve op til kommunens krav om informations- og forsyningssikkerhed.
(Se afsnit 3.6 *Leverandørscreening*.)

2.4 Kontraktforhandling og indgåelse

Kontrakten færdiggøres og sikrer, at:

- Identificerede krav indgår
- Roller, ansvarsfordeling og kommunikationsveje er tydeligt beskrevet
- SLA'er og krav til rapportering, hændelseshåndtering og revision er klart defineret
- Forhold vedr. databehandling (hvis relevant) er i fuld overensstemmelse med GDPR

En stærk kontrakt er afgørende for, at kommunen kan føre effektivt tilsyn og reagere, hvis sikkerhedskrav ikke overholdes.

2.5 Opdatering af leverandøroversigt

Når kontrakten er underskrevet, opdateres kommunens leverandøroversigt med relevante oplysninger, herunder:

- Leverandørens navn og kontaktoplysninger
- Kritikalitetsniveau
- Kort beskrivelse af leverancen
- Risikovurdering
- Gældende kontrakter og udløbsdatoer

(Se afsnit 3.7 *Leverandøroversigt*.)

Under kontrakt – Fase 3–5

I denne fase fokuserer kommunen på løbende styring, opfølgning og risikohåndtering i hele kontraktens løbetid. Vejledning til NIS2-loven "Implementering af cybersikkerhedsforanstaltninger" afsnit 4 - Forsyningskædesikkerhed understreger, at enheden bør sikre, at leverandører opretholder passende sikkerhedsforanstaltninger gennem SLA'er og revisionsmekanismer.

For at kunne opnå det fulde billede over leverandører, løsninger og tjenesteydelser er der behov for at identificere alle leverandører. Til brug for dette er udarbejdet "Guide til identifikation af kritiske leverandører".

Mængden af aktiviteter afhænger af leverancens karakter og risikoprofil – særligt om leverancen udgør et net- og informationssystem, og om sikkerhedskravene vedrører leverandørens produktion, selve løsningen eller begge dele.

3.1 Risikovurdering

Der gennemføres løbende risikovurderinger i overensstemmelse med kommunens risikostyringsproces, som identificeret i drejebogens kapitel vedr. Risikovurdering i afsnit 2.3.3 – "Frekvens for risikovurderinger".
Risikovurderingen kan føre til:

- Opdaterede sikkerhedskrav
- Yderligere kontroltiltag
- Justering af samarbejdet eller eskalering
- Inddragelse af kontrakt- eller leverandørstyringsfunktioner ved væsentlige fund

Det primære formål er at sikre at foranstaltninger står i rette forhold til risikovurderingen og dermed, at sikkerhedsforanstaltningerne fortsat er tilstrækkelige til, at kommunen kan efterleve NIS2.

4.1 Løbende monitorering

Vejledning til NIS2-loven "Implementering af cybersikkerhedsforanstaltninger" afsnit 4 – Forsyningskædesikkerhed stiller krav om at kommunen bør sikre sig at direkte leverandører og udbydere opretholder passende foranstaltninger. På baggrund heraf sikrer den ansvarlige for kontrakten løbende opfølgning på leverandørens efterlevelse af sikkerhedskrav og driftsforpligtelser gennem:

SLA-overvågning

Gennemgang af driftsrapporter og servicekvalitet Oppetid, svartider, løsningstider, registrering og opfølgning på afvigelser dokumenteres

Hændelsesovervågning

Leverandøren skal kontraktligt informere om relevante sikkerhedshændelser. Kommunen vurderer hændelsens påvirkning og behov for afhjælpning eller yderligere tilsyn

4.2 Revision og audit

Sikkerhedsrapportering

- Indhentning af årlige eller halvårlige sikkerheds- eller revisionsrapporter.
- Opdaterede certifikater (fx ISO 27001)
- Sikkerhedsspørgeskemaer eller interne/eksterne auditrapporter

Afhængig af leverandørens og/eller leverancens kritikalitet føres regelmæssigt tilsyn med leverandørens efterlevelse af kontraktens forhold. Det kan fx være igennem indhentning og gennemgang af ISAE3000 og/eller ISAE3402 erklæring eller tilsvarende fra leverandøren for at verificere sikkerhedstiltag. Der følges op på identificerede afvigelser og disse dokumenteres.

5.1 Opfølgning på kontrakt

Såfremt 3.1 – risikovurdering og 4.1 – løbende monitorering og 4.2 – revision og audit giver anledning til at skærpe kravene overfor leverandøren, kan det være nødvendigt at opdatere leverancens kontraktuelle betingelser. Såfremt de ændrede forhold ikke kan afspejles i en opdateret kontrakt er det essentielt at dokumentere overvejelserne forbundet med beslutningen.

Efter kontrakt – fase 6

Når en leverandørkontrakt udløber eller opsiges, bør kommunen sikre en kontrolleret afvikling af samarbejdet.

Mængden af aktiviteter og foranstaltninger vil variere afhængig af, om det alene er leverandørens eget produktions- og leveranceapparat der stilles informations- og cybersikkerhedskrav til, og/eller det også vedrører selve leverancen – hvis denne er af typen net- og informationssystem.

6. Nedlukning af leverancen

Ved ophør af samarbejdet gennemføres en kontrolleret udfasning, som omfatter:

- Afslutning af adgangsrettigheder
- Sikret overførsel eller sletning af data
- Dokumentation af afslutningen
- Evaluering af leverandørens samlede performance
- Opdatering af leverandøroversigten med ophørsdato

Formålet er at sikre, at kommunen ikke efterlader åbne risici, og at afslutningen sker i overensstemmelse med både kontrakt og sikkerhedskrav. Der kan findes inspiration til den obligatoriske procedure for leverandørstyring i det kommunale eksempel "Disposition til procedure for leverandørstyring".

Med udgangspunkt i leverandørcyklussens enkelte faser, som beskrevet ovenfor, gennemgås udvalgte områder nærmere i de efterfølgende afsnit. Afsnittene skal ses som inspiration. Den beskrevne metode og de listede krav kan udvides eller adopteres helt eller delvist. Det vigtigste er, at I som kommune har forholdt jer til faserne og at I får det afspejlet i jeres procedure for leverandørstyring på et realistisk niveau, så både procedure og de listede leverandørkrav har et risikobaseret udgangspunkt og kan blive implementeret og efterlevet. Se eksempel i "Disposition til procedure for leverandørstyring".

Med det øgede fokus og de skærpede krav vil både jeres og leverandørernes modenhed øges og I bør derfor løbende vurdere, om proceduren og leverandørkravene skal skærpes - bl.a. med udgangspunkt i det aktuelle trusselsbillede.

3.3 Behovsafdækning og initiel vurdering

Når kommunen skal anskaffe et nyt system eller tjeneste skal det kortlægges, hvorvidt løsningen eller tjenesten understøtter en eller flere kritiske processer i kommunen. På baggrund af den vurderede kritikalitet, har man en initial vurdering af, hvilket kravniveau der skal pålægges leverandøren, der omfatter de foranstaltninger, der følger af NIS2. Det giver kommunen et pejlemærke af, hvor risikobetonet anskaffelsen er.

I kapitel 2 - Risikostyring, afsnit 2.4 findes hjælp til at identificere kritiske processer, systemer og tjenester. Det vil sige at når kommunen har gennemført den proces, findes der er et overblik over kommunens kritiske processer.

Afsnittet beskriver fase 1 i leverandørcyklus.

Guide til identifikation af kritiske processer

Kortlægning

Risikostyring

Leverandørstyring

Hændelshåndtering

Fremgangsmåde Step-by-step

1. Udvælg område fra "Kommunernes opgaver"
2. Identificér underliggende processer
3. Identificér herunder de kritiske processer
   - Se "Fase 3 – identifikation af kritiske processer og opgaver".
4. Identificér den underliggende systemunderstøttelse til den kritiske proces
   - Se "Fase 4 – Identifikation af systemer, der understøtter de kritiske processer"
5. Identificér de kritiske infrastruktur komponenter
   - Se "Fase 5 – Identificér underliggende infrastrukturkomponenter
6. Identificér kritiske integrationer
   - Se "Fase 6 – Identificér kritiske integrationer"

Model 2.4.1

3.4 Kritikalitets og risikovurdering af leverandører

Jf. vejledning til NIS2-loven om implementering af cybersikkerhedsforanstaltninger, bør kommunen anvende en risikobaseret tilgang, hvor kravene til den enkelte leverandør eller tjenesteudbyder er proportional med den specifikke leverances betydning for kommunens forsynings- og cybersikkerhed ud fra et NIS2-perspektiv, for at undgå unødigt høje krav. Dette betyder, at kravene til leverandører differentieres efter den kritikalitet, som den enkelte leverance har for kommunens opgavevaretagelse. Dette sikrer både en effektiv ressourceudnyttelse og en proportional sikkerhedsstyring, hvor de mest kritiske leverancer, i et NIS2 perspektiv, får den nødvendige opmærksomhed, mens mindre kritiske leverancer håndteres med standardiserede processer, som dog stadig afspejler, at kommunen som helhed er underlagt NIS2. Afsnittet beskriver fase 2 i leverandørcyklussen.

I drejebogens kapitel 2 - Risikostyring har kommunen ved hjælp af afsnit 2.4 "Guide til identifikation af kritiske processer, systemer og tjenester" kortlagt hvilke processer, systemer mv. der er kritisk for kommunen. Med udgangspunkt heri kan kommunen knytte leverandører til de forskellige løsninger og kommunen har hermed en delmængde af deres leverandører. For en fuldkommen kortlægning tages udgangspunkt i den restmængde (de mindre kritiske) af opgaver/processer som ikke allerede er behandlet. Det er vigtigt at have et samlet overblik over alle de leverancer en leverandør har til kommunen, for at kunne sikre at alt er risikovurderet.

For at kunne stille de rigtige krav til leverandører vurderes herefter kritikalitetsniveau. Kritikalitets- og risikovurderingen er en dynamisk proces, der gentages med regelmæssige intervaller gennem hele kontraktperioden.

Formålet med den løbende kritikalitets- og risikovurdering er at sikre, at kommunens forståelse af leverandørens betydning og risikoprofil forbliver aktuel, og at eventuelle ændringer i enten leverandørens situation eller kommunens afhængighed opdages og håndteres proaktivt. Leveran-dører kan ændre sig over tid - gennem opkøb, strategiskift, organisatoriske forandringer eller ændringer i deres økonomiske situation - og kommunens afhængighed kan ligeledes udvikle sig, hvis leverancen udvides eller integreres dybere i kommunens processer.

Vurderingsprocessen følger 5-trin, beskrevet i nedenstående "Guide til identifikation af kritiske leverandører".

3.4.1 Guide til identifikation af kritiske leverandører

Guide til identifikation af kritiske leverandører

Fremgangsmåde Step-by-step

1. Kortlægning af leverandører + kobling til kritiske processer/systemer
2. Identificér løsninger/ydelser pr. leverandør
3. Kritikalitetsvurdering
4. Substituerbarhedsvurdering
5. Handlingsplan

Model 3.4.1

I den efterfølgende gennemgang af trin 1-5 i modellen og der henvises til "Guide til identifikation af kritiske leverandører" for eksempler.

Trin 1-2: Kortlægning af leverandører og løsninger

For at imødekomme kravet om en risikobaseret tilgang til leverandørstyring kræver det at kommunen har et komplet overblik over alle leverandører og de specifikke løsninger, som hver leverandør leverer til kommunen. Dette er fundamentet for den videre vurdering.

Det er vigtigt at opdele leverandørens samlede leverance i specifikke løsninger, da samme leverandør ofte leverer services med forskellig kritikalitet. Kommunen har ved hjælp af " Guide til identifikation af kritiske processer, understøttende systemer, infrastruktur og integrationer " i kapitel 2 vedr. Risikovurdering kortlagt hvilke kritiske processer, understøttende systemer, infrastruktur og integrationer, hvilke i dette trin skal have tilknyttet den pågældende leverandør.

Trin 3: Kritikalitetsvurdering

I Trin 2 har kommunen allerede kortlagt, hvad der er kritisk, men ikke hvor kritisk. Dette er vigtigt at kortlægge for at kunne stille risiko-baserede krav til leverandørerne.

Kritikalitetsvurderingen sker på baggrund af IT-løsningens samfundskritikalitet, det vi sige, hvor vigtig er IT-løsningen for kommunens opgave-varetagelse.

Samfundsskritikaliteten anvender kategorierne K1 (lav), K2 (middel), K3 (høj) og K4 (kritisk) til at beskrive den aktuelle kritikalitet. Kategorierne er valgt på baggrund af SKI's scoringsmodel for kritikalitet, således at vurderingen kan anvendes som vejledende redskab, når der skal udvælges hvilke krav der skal stilles til leverandøren i SKI's kravkatalog(se afsnit 3.5)

Kritikalitetsvurderingen tager udgangspunkt i spørgsmål som: Hvilke kritiske processer påvirkes ved svigt? Kan lovpligtige opgaver opretholdes? Hvad er konsekvensen for borgere ved nedbrud? Hvor lang nedbrudstid kan tolereres? Se konsekvensniveauer i kapitel 2 vedr. Risikovurdering i afsnit 2.3.1 "Risikovurderingsramme".

Trin 4: Substituerbarhedsvurdering
Substituerbarhedsvurderingen er en vurdering af, hvor let eller svært det er for en organisation at substituere en leverandør, system eller løsning med et alternativ. Kritikaliteten af en leverandør afhænger derfor ikke kun af leverancens betydning, men også af hvor let eller svært det er at substituere leverandøren.

En leverance kan være højkritisk for kommunens drift på et område der er kritisk for samfundet, men hvis der findes flere alternative leverandører på markedet, reduceres den samlede risiko betydeligt. Omvendt skaber kombinationen af høj kritikalitet og lav substituerbarhed særlig sårbarhed.

Substituerbarheden vurderes primært ud fra den tid, det realistisk vil tage at skifte leverandør. Der er visse særlige opmærksomhedspunkter ved substituerbarhedsvurderingen såsom at Fælleskommunale løsninger som KOMBIT-løsninger ofte har lav substituerbarhed, men til gengæld højere forsyningssikkerhed gennem fælles governance. Cloud-hyperscalere har lav substituerbarhed grundet dyb integration, men ofte høj stabilitet. Niche-leverandører indebærer risiko for virksomhedsophør, opkøb eller strategiskift.

Trin 5: Handlingsplan
Baseret på kombinationen af kritikalitet og substituerbarhed defineres en konkret handlingsplan for den enkelte leverandør. Handlingsplanen indebærer også at vurdere, hvilke krav der skal stilles til leverandøren. Leverandører med høj kritikalitet og lav substituerbarhed udgør den største risiko og kræver omfattende kontraktuelle krav, løbende kontrol og kontinuitetsplanlægning.

Revurdering af kritikalitet
Frekvensen for revurdering afhænger af leverandørens kritikalitet:

- For K3/K4-leverandører gentages vurderingen mindst årligt eller ved væsentlige ændringer.
- For K2-leverandører foretages vurdering ved kontraktfornyelse eller ved væsentlige ændringer
- K1-leverandører vurderes ad hoc.

Resultatet af kritikalitets- og risikovurderingen dokumenteres i kommunens leverandøroversigt, som dermed giver det samlede overblik over alle leverandører med tilhørende kritikalitet, substituerbarhed og handlingsplan.

3.5 Guide til bestemmelse af differentierede krav

Jf. vejledning til NIS2-loven om implementering af cybersikkerhedsforanstaltninger, bør kommunen anvende en risikobaseret tilgang, hvor kravene til den enkelte leverandør eller tjenesteudbyder er proportional med den specifikke leverances betydning for kommunens forsynings- og cybersikkerhed, for at undgå unødigt høje krav. Dette betyder, at kravene til leverandører differentieres efter den kritikalitet, som den enkelte leverance har for kommunens opgavevaretagelse. Dette sikrer både en effektiv ressourceudnyttelse og en proportional sikkerhedsstyring, hvor de mest kritiske leverancer får den nødvendige opmærksomhed, mens mindre kritiske leverancer håndteres med standardiserede processer. Afsnittet beskriver leverandørcyklussens fase 2.

Differentieringen af krav tager udgangspunkt i kritikalitets- og risikovurdering af den konkrete leverandør og leverance gennem metoden beskrevet i "Guide til identifikation af kritiske leverandører" (fase 3 – Kritikalitetsvurdering). Når leverancens kritikalitet er fastlagt gennem metoden i "Guide til identifikation af kritiske leverandører", vælger kommunen de passende krav, der matcher leverancens betydning.

Det væsentligste er dog, at kravene dækker NIS2-lovens ti cybersikkerhedsforanstaltninger (§6, stk. 1) og er differentieret efter leverancens kritikalitet.

De ti foranstaltninger

1. Politikker for risikostyring og informationssikkerhed (§ 6, stk. 1, nr. 1)
2. Håndtering af hændelser (§ 6, stk. 1, nr. 2)
3. Driftskontinuitet og krisestyring (§ 6, stk. 1, nr. 3)
4. Kædeansvar/leverandørsikkerhed (§ 6, stk. 1, nr. 4)
5. Erhvervelse, udvikling og vedligeholdelse (§ 6, stk. 1, nr. 5)
6. Vurdering af sikkerhedsforanstaltningers effektivitet (§ 6, stk. 1, nr. 6)
7. Grundlæggende Cyberhygiejne og Awareness (§ 6, stk. 1, nr. 7)
8. Brug af kryptografi (§ 6, stk. 1, nr. 8)
9. Personalesikkerhed, adgangsstyring og forvaltning af aktiver (§ 6, stk. 1, nr. 9)
10. Multifaktor autentifikation og sikker kommunikation (§ 6, stk. 1, nr. 10)

Kilde: NIS2-loven

3.5.1 Bestemmelse af krav

Kravene til leverandører i drejebogen er opdelt i fire kategorier baseret på kritikalitetsniveau. Opdelingen skal betragtes som et forslag til en mulig metode. Kommunen vurderer selv, om den understøtter de eksisterende arbejdsgange eller om en allerede etableret metode er mere hensigtsmæssig.

Betegnelsen K1-K4 (Kritikalitet 1-4) er valgt for at skabe sammenhæng med SKI's eksisterende kritikalitetsmodel, som kommunerne allerede anvender i deres indkøbsprocesser. Ved at anvende samme notation sikres en ensartet tilgang på tværs af kommunens leverandørstyring, uanset om leverancen sker gennem SKI-aftaler eller andre indkøbskanaler. Dette letter kommunikationen med både interne interessenter og eksterne leverandører, der ofte er bekendt med SKI's kategorisering. Det står dog kommunerne frit for at anvende egne metoder

De fire kritikalitetsniveauer

K4 – Kritisk

Leverancer med vital betydning for kommunens samfundskritiske opgavevaretagelse eller borgersikkerhed kræver de mest omfattende sikkerhedskrav. For disse leverandører anbefales at kontrakten som minimum indeholder krav om dokumenteret informationssikkerheds-styring baseret på anerkendte standarder (fx ISO-27001 eller tilsvarende), ret til sikkerheds audit, incident-notifikation indenfor 24 timer, dokumenterede business continuity plans samt krav om forudgående godkendelse af underleverandører. Den løbende opfølgning omfatter kvartalsvis performance review og årligt tilsyn.

K3 - Høj kritikalitet

Leverancer med høj betydning for centrale kommunale opgaver stilles overfor samme kravniveau som K4-leverancer, da kombinationen af høj kritikalitet og potentielt store konsekvenser ved svigt kræver maksimal sikring.

K2 - Middel kritikalitet

Leverancer med middel kritikalitet håndteres med standardiserede sikkerhedskrav, herunder grundlæggende sikkerheds-dokumentation, SLA med minimum 99% oppetid, notifikation om hændelser inden 48 timer samt dokumenterede backup-procedurer. Den løbende opfølgning omfatter halvårlig gennemgang og årlig opfølgning på NIS2 compliance.

K1 - Lav kritikalitet

Leverancer med lav kritikalitet håndteres med standard kontraktvilkår og grundlæggende SLA, med ad hoc gennemgang ved kontraktfornyelse.

Metode
Selvom kravkategorierne K1-K4 giver overordnede retningslinjer, skal de konkrete sikkerhedskrav altid tilpasses den enkelte leverances specifikke risikoprofil. Jf. Kommunens politik for risikostyring, foretages risikovurderinger af hver leverance for at sikre, at kravene er proportionale og relevante.

Det konkrete indhold af sikkerhedskravene til leverandører kan tage udgangspunkt i SKI's kravkatalog til IT-konsulentydelser (Materiale fra SKI - Sikkerhedskrav, tilgængeligt på www.ski.dk), som mange kommuner allerede anvender i deres indkøbsprocesser. SKI's kravkatalog er struktureret i pakker (B, 1, 2, 3) med tilhørende tillægspakker og dækker de væsentligste sikkerhedsområder.

For leverancer der ikke indkøbes på SKI-aftaler, kan kommunen anvende SKI's kravkatalog som inspiration eller udgangspunkt og tilpasse kravene til den konkrete leverancesituation. Alternativt kan kommunen anvende andre kravkataloger baseret på anerkendte standarder som ISO 27001 eller lignende.

Ved nye anskaffelser indarbejdes de relevante sikkerhedskrav i udbudsmaterialet og kontrakten fra starten.

Ved gennemgang af eksisterende kontrakter kan der udarbejdes en GAP-analyse med udgangspunkt i SKI's kravkatalog. Formålet er at vurdere, om kontrakten indeholder de nødvendige sikkerhedskrav i forhold til leverancens og leverandørens kritikalitet. Samt om der eventuelt er behov for at genforhandle eller ajourføre kontraktgrundlaget.

Der vil være tilfælde hvor det ikke er muligt at genforhandle en kontrakt i kontraktperioden. Her dokumenteres overvejelserne for de enkelte løsninger og handleplan for sikring af at kravene ændres, en kontrakt genforhandles eller løsningen udbydes på ny.

Den differentierede tilgang sikrer, at kommunen kan fokusere ressourcerne på de leverancer, hvor risikoen er størst, mens mindre kritiske leverancer håndteres effektivt gennem standardiserede processer.

3.6 Leverandørscreening

I vejledning til NIS2-loven "Implementering af cybersikkerhedsforanstaltninger" står angivet at kommunen bør definere kriterier for, hvordan de udvælger leverandører eller tjenesteudbydere. Til at understøtte dette arbejde er der udarbejdet en model som uddybes nedenfor. Afsnittet beskriver leverandørcyklussens fase 2.

Før kommunen indgår kontrakt med en ny leverandør, er det vigtigt at gennemføre en systematisk screening af leverandøren for at sikre, at leverandøren har de nødvendige kapabiliteter og ressourcer til at leve op til kommunens krav. Leverandørscreeningen fungerer som en forhåndsvurdering af leverandøren, der giver kommunen et grundlag for at vurdere, om leverandøren er egnet som samarbejdspartner. Screeningsmodellen er inspireret af SKI's due diligence-praksis og tilpasset til NIS2-krav.

Det er vigtigt at præcisere, at formålet med modellen for leverandørscreening ikke er at gennemføre en fuldstændig vurdering af leverandørens efterlevelse af NIS2-kravene.

Modellen fungerer derimod som et værktøj til at vurdere, om leverandørens kapabiliteter gør denne egnet til at levere ydelser til kommunen.

Screeningsprocessen gennemføres typisk, når kommunen har identificeret en foretrukken leverandør, men inden den endelige kontraktindgåelse. Formålet er at afdække eventuelle risikofaktorer tidligt i processen og sikre, at leverandøren matcher kommunens forventninger på områder som compliance, informationssikkerhed, økonomisk stabilitet og organisatorisk kapacitet.

I det følgende gennemgås modellens struktur og anvendelse.

3.6.1 Overblik

Som udgangspunkt udfylder kommunen de grundlæggende oplysninger, herunder leverandørens navn, dato for udfyldelse, navn på den person, der har gennemført screeningen, samt den vurderede kritikalitet for leverandøren. Kritikaliteten hentes fra "Guide til identifikation af kritiske leverandører" (jf. tidligere forklaring i afsnit 3.4.1) og har betydning for, hvilke score der anses som acceptabel for den pågældende leverandør.

Kolonnen *"Score"* fungerer som en støtte for udfylderen og anvendes i forbindelse med den efterfølgende scoring af leverandøren.
Det er vigtigt at bemærke, at kun de blå markerede felter skal udfyldes.

Leverandørnavn:	Dato:	Udfyldt af:	Kritikalitet	Score
(Indsæt leverandørnavn her)	*(Indsæt dato)*	*(Indsæt navn)*	*(Indsæt kritikalitet pba vurdering)*	4: Fremragende 3: God 2: Acceptabel 1: Svag N/A: Ikke relevant for anskaffelsen
Skal udfyldes		*Skal ikke udfyldes*		

Model 3.6.1.1

3.6.2 Scoring

Screeningen tager udgangspunkt i en struktureret model, der vurderer leverandøren på seks centrale områder.

Compliance: Vurdering af om leverandøren kan efterleve relevante lovkrav og standarder, herunder muligheden for at indgå databehandleraftale, etablering af procedurer for NIS2-compliance, og om der sker overførsel af data til usikre tredjelande.

Informationssikkerhed: Vurdering af leverandørens sikkerhedsniveau, herunder dokumenteret informationssikkerhedspolitik baseret på anerkendte standarder (fx ISO 27001), tilsynsmuligheder i kontrakten, procedurer for hændelseshåndtering samt regelmæssige risikovurderinger og tekniske tests.

Kapacitet og robusthed: Vurdering af leverandørens evne til at levere stabilt under spidsbelastning, dokumenteret beredskabsplan for driftskontinuitet samt backup og gendannelsestest.

Økonomi: Vurdering af leverandørens økonomiske stabilitet gennem soliditets- og likviditetsgrad samt tegning af relevante forsikringer. En økonomisk sund leverandør mindsker risikoen for pludseligt leverandørsvigt.

Underleverandører: Vurdering af leverandørens brug af underleverandører og de processer, der sikrer, at underleverandører overholder relevante krav gennem løbende kontrol og tilsyn.

CSR: Vurdering af leverandørens Code of Conduct og politikker for bæredygtighed og socialt ansvar. CSR-forhold indgår ofte i kommunale indkøbspolitikker og er derfor medtaget i screeningsmodellen.

Scoringen foretages på en skala fra 1 til 4, hvor 1 angiver den laveste og 4 den højeste vurdering (jf. afsnit 3.5.1). Hvis et spørgsmål vurderes ikke at være relevant for den pågældende leverandør, angives det som *N/A*.

For kategorien "Økonomi" kan der hentes støtte i fanen "Vejledning", hvor der fremgår en oversigt over de forventede intervaller for relevante nøgletal.

Det anbefales at tilføje en kommentar til hvert enkelt spørgsmål for at dokumentere de overvejelser, der ligger til grund for den tildelte score

Kategori	Spm.	Spørgsmål	Score (1-4)	Noter/dokumentation
A. Compliance (vægt 20)				
	1	Er der mulighed/behov for indgåelse af databehandleraftale?	0	
	2	Har leverandøren etableret procedurer for at opfylde NIS2-krav og/eller andre relevante standarder?	0	
	3	Overføres der data (både personoplysninger og forretningskritiske) til usikre tredjelande	0	
B. Informationssikkerhed (vægt 30)				
	1	Har leverandøren en dokumenteret informationssikkerhedspolitik baseret på en anerkendt standard (fx ISO 27001)?	0	
	2	Hvilke tilsynsmuligheder er det muligt at indarbejde i kontrakten, som sikrer I løbende overholdelse af lovgivning og standarder (fx interne audits, revisionserklæringer)?	0	
	3	Har leverandøren en formel og ledelsesgodkendt procedure for håndtering af hændelser og testes denne jævnligt?	0	
	4	Udfører leverandøren regelmæssige risikovurderinger og tekniske tests (kan være penetrationstests og sårbarhedsscanninger)?	0	
C. Kapacitet & robusthed (vægt 15)				
	1	Har leverandøren kapacitet til at levere stabilt under spidsbelastning, og hvordan dokumenteres dette	0	
	2	Har leverandøren en beredskabsplan for driftskontinuitet, herunder backup og dokumenteret gendannelsestest og er kommunikation og koordination med kunder indtænkt i tilstrækkelig grad?	0	
D. Økonomi (vægt 15)				
	1	Er leverandørens soliditets- og likviditetsgrad tilfredsstillende (undersøg gerne de sidste tre år)?	0	
	2	Hvilke forsikringer har leverandøren tegnet, herunder professionel ansvarsforsikring?	0	
E. Underleverandører (vægt 10)				
	1	Benytter leverandøren underleverandører, og hvordan sikres, at de overholder relevante krav og lovgivning?	0	
	2	Har leverandøren en proces for løbende kontrol og tilsyn med deres underleverandører?	0	
F. CSR (vægt 10)				
	1	Har leverandøren en Code of Conduct og politikker for bæredygtighed og social ansvarlighed, og kan implementeringen dokumenteres?	0	

Model 3.6.2.1

3.6.3 Samlet score

Når alle spørgsmål er blevet vurderet, beregner modellen en samlet score for leverandøren baseret på en vægtning af de seks spørgsmåls-kategorier. Vægtningen angiver den relative betydning af hver kategori i forhold til kommunens samlede vurdering. Modellen indeholder en standardvægtning for hver kategori, men det er op til kommunen at vurdere, om denne vægtning afspejler kommunens risikoprofil. Kommunen kan selv justere vægtningen i modellen.

Foretages der ændringer, skal kommunen sikre, at formlerne i cellerne E30–E35 opdateres tilsvarende.

Hver kategori tildeles point baseret på leverandørens svar og dokumentation, og den samlede score sammenholdes med leverancens kritikalitetsniveau for at afgøre, om leverandøren vurderes som egnet. Som udgangspunkt skal leverandører til K1-leverancer score mellem 50-60 point, K2-leverancer mellem 60-75 point, K3-leverancer mellem 70-85 point og K4-leverancer over 85 point.

Derudover skal tre "minimumskrav" være opfyldt: informationssikkerhedspolitik, dokumenteret hændelseshåndtering og tilfredsstillende økonomi.

Kategori-sammendrag			Vægt	
A. Compliance			20	-
B. Informationssikkerhed			30	-
C. Kapacitet & robusthed			15	-
D. Økonomi			15	-
E. Underleverandører			10	-
F. CSR			10	-
Samlet score				-

Model 3.6.3.1

3.6.4 Minimumskrav

Som navnet angiver, udgør minimumskrav, det der skal være opfyldt, for at en leverandør kan kvalificere sig til at indgå kontrakt med kommunen. Det forventes derfor som udgangspunkt, at alle spørgsmål i denne kategori kan besvares med "ja".

Hvis kommunen vurderer, at yderligere elementer bør indgå som *minimumskrav*, kan disse tilføjes i modellen. En sådan tilpasning kræver ingen konsekvensrettelser i beregningerne, men det anbefales, at ændringerne dokumenteres for at sikre sporbarhed og gennemsigtighed.

Minimumskrav (skal være 'Ja')		Svar (Ja/Nej)		Noter/dokumentation
Informationssikkerhedspolitik		Ja		
Dokumenteret hændelseshåndtering		Nej		
Tilfredsstillende økonomi		Ja		

Model 3.6.4.1

3.6.5 Samlet vurdering af leverandør

Resultatet af screeningen giver kommunen et klart billede af leverandørens styrker og svagheder og danner grundlag for en beslutning om, hvorvidt kontraktforhandlinger skal fortsættes, eller om der er behov for at stille supplerende krav til leverandøren som betingelse for kontraktindgåelse.

Når kommunen vurderer, hvorvidt den samlede score er tilfredsstillende i forhold til leverandørens vurderede kritikalitet, anvendes nedenstående skema. Det vil sige at forventningen til den samlede score er proportionel med leverandørens kritikalitet for kommunen. Som det ses af model 3.6.5.1, anbefales det ikke at acceptere leverandører med en score under 50.

Hvis vurderingen ikke anses for tilfredsstillende af kommunen, kan der aftales nødvendige forbedringstiltag, samt fastsættes frister for udbedring. Dette dokumenteres i modellen under "Påkrævede forbedringer og frister". Disse tiltag kan efterfølgende indgå som en del af den samlede vurdering af leverandøren

Hvis screeningsresultatet viser betydelige mangler i forhold til leverancens kritikalitet, kan kommunen også vælge at søge alternative leverandører

Screeningsskabelonen med tilhørende vejledning og eksempel findes i "Leverandørscreening". Her opsummeres en samlet vurdering af leverandøren baseret på den samlede score og minimumskrav.

Egnethedsvurdering:	Vurderes egnet K1: score mellem 50 - 60 K2: score mellem 60 - 75 K3: score mellem 70 - 85 K4: score mellem over 85 + ja i alle musthaves gælder for alle

Model 3.6.5.1
På den sidste fane i skabelonen findes et eksempel

3.6.6 Dispensationer

Leverandørscreeningen anvendes som grundlag for vurdering af den enkelte leverandør og dokumentation for efterlevelse af kravet om kriterier for udvælgelse af leverandører eller tjenesteudbydere. Selvom en leverandør-screenings resultat ikke er tilfredsstillende og ikke ligger indenfor de tærskelværdier kommunen har angivet, kan vurderingen stadig falde positivt ud for leverandøren. Her anbefales det dog, at man er særlig opmærksom på at dokumentere de yderligere overvejelser, der ligger til grund for at indgå kontrakt med leverandøren og følge kommunens proces for dispensationer.

3.7 Leverandøroversigt

For at kunne efterleve kravet om, at kommunen bør sikre at direkte leverandører og udbydere, herunder cloud-computing udbydere, opretholder passende foranstaltninger er det nødvendigt med et fuldkomment overblik over alle kommunens leverandører og tjenesteudbydere. På baggrund heraf er udarbejdet en template til overblik over kommunens leverandører.

For at kommunen kan opfylde dokumentations- og overblikskravene i NIS2, er det nødvendigt at etablere et centralt register over alle leverandører med tilhørende kritikalitets- og risikovurderinger. Dette register fungerer både som et styringsværktøj i det daglige arbejde og som dokumentation over for tilsynsmyndigheden.

Der er udarbejdet en Excel-baseret skabelon til leverandøroversigt, som håndterer de komplekse sammenhænge mellem leverandører, systemer, processer og kritikalitetsvurderinger. Skabelonen findes i to versioner: en "light-model" og en ”detaljeret-model". Begge modeller er i drejebogen opbygget i Excel. Såfremt kommunen ønsker at værktøjsunderstøtte leverandøroversigten, kan begge modeller anvendes som inspiration hertil.

3.7.1 Light-model

”Light-modellen” er den anbefalede version for de fleste kommuner og fokuserer på de væsentligste oplysninger, som er nødvendige for at opfylde NIS2-kravene og sikre effektiv leverandørstyring. Light-modellen indeholder to hovedark:

Leverandører: Denne fane indeholder en oversigt over alle kommunens leverandører med grundlæggende information som leverandørnavn, CVR-nummer, leverandørtype, antal systemer/løsninger, højeste kritikalitet, kontaktoplysninger samt ansvarlige i kommunen. For hver leverandør angives den højeste kritikalitet blandt leverandørens løsninger, så kommunen hurtigt kan identificere de mest kritiske leverandører.

Systemer og løsninger: Denne fane opdeler hver leverandørs leverance i specifikke systemer og løsninger med tilhørende kritikalitetsvurdering, kobling til kritiske processer, substituerbarhed samt handlingsplan. Dette ark er kernen i leverandørstyringen, da det er her, den detaljerede vurdering af den enkelte løsning foretages og handlingsplanen defineres.

Skabelonen er designet med indbyggede relationer mellem arkene, så oplysningerne automatisk opdateres på tværs. Når en løsnings kritikalitet opdateres i "Systemer og løsninger"-arket, opdateres leverandørens samlede kritikalitet automatisk i "Leverandører"-arket.

Skabelonen til ”Leverandøroversigt – light” findes her

3.7.2 Detaljeret-model

Den detaljerede model indeholder yderligere ark til mere detaljeret håndtering af mange-til-mange-relationerne mellem leverandører, systemer og processer. Denne version er relevant for større kommuner med komplekse leverandørlandskaber eller for kommuner, der ønsker et mere granuleret styringsniveau.
Den detaljerede model er dog mere ressourcekrævende at vedligeholde.

For de fleste kommuner anbefales det at starte med light-modellen, da den giver det nødvendige overblik og styringsgrundlag uden at skabe unødig administration. Skabelonen kan tages i brug gradvist, ved at kommunen starter med at kortlægge de mest kritiske leverandører og løbende udvider registeret.

Det er vigtigt, at ansvaret for vedligeholdelse af leverandøroversigten er klart defineret i kommunen. Typisk vil dette ansvar ligge hos IT-afdelingen i samarbejde med indkøbsfunktionen, men den konkrete organisering afhænger af kommunens størrelse og struktur. Det væsentlige er, at oversigten holdes ajour, så den til enhver tid afspejler kommunens faktiske leverandørlandskab og risikovurderinger.

Skabelonen til "Leverandøroversigt – detaljeret" findes her

3.8 Definitioner

Nedenstående afsnit er en hjælp til læseren for sikring af en ensartet forståelse af begreberne i drejebogens kapitel 3 - Forsyningskædesikkerhed

- **Samfundskritikalitet** - Løsningens betydning for kommunens opgavevaretagelse
- **Substituerbarhed** – I hvilken grad et IT-system eller leverandør kan erstattes af et andet IT-system eller leverandør inden for en acceptabel tid og uden væsentlig påvirkning af kommunens kritiske processer.

Bilag 3a Oversigt over centrale krav til forsyningskædesikkerhed

Juridisk grundlag
Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven), vedtaget 29. april 2025, trådte i kraft 1. juli 2025. Gælder for kommuner, der er identificeret som væsentlige eller vigtige enheder jf. § 4 og § 5 i loven.

Centrale paragraffer i NIS2-loven vedr. risikostyring

§	Krav	Kravstype	Indhold
§ 6, stk. 1, nr. 4	Enheden skal implementere forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem enheden og dens direkte leverandører eller tjenesteudbydere.	Skal	Forpligtelse til at sikre, at leverandører og tjenesteudbydere har passende sikkerhedsforanstaltninger, og at relationerne dokumenteres og styres i et risikobaseret setup.

Centrale krav til risikostyring i NIS2-direktivet

Artikel	Krav	Kravstype	Indhold
Artikel 20, stk. 2, d	Enheden skal gennemføre foranstaltninger vedrørende "supply chain security.	Skal	Enheder skal vurdere sårbarheder i leverandørkæden, leverandørens sikkerhedspraksis, produktkvalitet og sikre passende tekniske, organisatoriske og kontraktuelle sikkerhedskrav.

Centrale vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIK's Vejledning til kommuner om NIS2-loven	Kommunen skal implementere procedurer leverandørstyring	Skal	Procedurer skal sikre forsynings- og cybersikkerhed i samarbejde med direkte leverandører eller tjenesteudbydere.
SAMSIK's Vejledning til Implementering af Cybersikkerhedsforan stalt-ninger	Enheden skal udarbejde en procedure for leverandørstyring	Skal	Proceduren skal sikre både forsyningssikkerhed og cybersikkerhed i samarbejdet med direkte leverandører eller tjenesteudbydere