NIS2-koncepter til kommunal implementering

Risikovurdering

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 tema-grupper 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 Risikovurdering
I dette kapitel af den kommunale NIS2-drejebog præsenteres en tilgang til arbejdet med NIS2-risikovurdering i kommunen. Risikovurdering er et bærende element i NIS2-implementering bl.a. da de centrale 10 foranstaltninger skal implementeres på passende niveau ud fra kommunens risikovurdering. Kommunens risikovurdering skal desuden være rettesnor for de krav, der stilles til kommunens direkte leverandører af it-systemer.

Ikke alle kommunens opgaver og it-understøttelse vil være lige kritiske – det skal der tages hensyn til i NIS2-implementeringen. Samtidigt skal der tages hensyn til systemers kritikalitet, hvor afhængigheden mellem systemer skal vurderes.

Drejebogsmateriale giver struktur og 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 Net- og 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. Eksempelvis sundhedsområdet, gør at kommunerne i NIS2 udpeges som væsentlig enhed.

Forord

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

Læsevejledning

Anvendelse af termer og referencer til NIS2. Dækker over referencer til både lovtekster og vejledninger fra SAMSIK.

1. **"Skal" – Juridisk bindende krav**
   - **Betydning**: Udtryk for en *pligt* eller et *ufravigeligt krav*.
   - **I NIS2 (direktiv og lov)**: Bruges til at angive krav, som enheder *skal* efterleve for at være i overensstemmelse med loven.
   - **Eksempel**: "Enheder skal implementere passende tekniske og organisatoriske foranstaltninger."
   - **Operationelt**: Skal omsættes til kontrollerbare handlinger og dokumenterbare procedurer. Typisk krav, der skal mappes direkte i Excel-ark og auditeres.

2. **"Bør" – Stærk anbefaling med forventning**
   - **Betydning**: Udtryk for en *forventning* eller *best practice*, som myndighederne *forventer* bliver fulgt, medmindre der er velbegrundede argumenter til andet.
   - **I NIS2 (direktiv og lov)**: Bruges ofte i vejledninger og fortolkninger, hvor der gives anbefalinger til opfyldelse af krav
   - **Eksempel**: "Ledelsen bør involveres aktivt i cybersikkerhedsstrategien."
   - **Operationelt**: Bør omsættes til governance-elementer, der kan dokumenteres og forklares i audit-sammenhæng. Kan indgå som anbefalede leverancer i PowerPoint til ledelsesforankring.

3. **"Kan" – Mulighed eller valgfrihed**
   - **Betydning**: Udtryk for en *valgmulighed*, typisk uden juridisk binding.
   - **I NIS2 (direktiv og lov)**: Bruges til at indikere fleksibilitet i metodevalg eller organisatorisk tilpasning.
   - **Eksempel**: "Enheder kan vælge at anvende en ekstern leverandør til risikovurdering."
   - **Operationelt**: Kan bruges til at dokumentere alternativer i leverandørstyring eller beredskabsplanlægning. Ikke krav, men relevante i strategiske overvejelser.

Ved **'anbefaler'**, er det drejebogens metode til at løse hhv. kan, bør og skal kravene, og altså ikke noget der skal ses som et krav, men et forslag eller metode til en måde at efterleve kravene.

2. Risikostyring under NIS2

Arbejdet med risikostyring skal tage afsæt i, at kommunerne, som væsentlige enheder defineret i § 4 i NIS2-loven, er forpligtet til at etablere og vedligeholde en systematisk, dokumenteret og risikobaseret tilgang til beskyttelse af net- og informationssystemer jf. § 6, stk. 1 i NIS2-loven.

Arbejdet med risikostyring bør være integreret i den samlede governance for informationssikkerhed og understøtte ledelsens beslutningsgrundlag, prioritering af ressourcer og dokumentation over for tilsynsmyndigheder.

Risikostyringen skal være operationel, dokumenteret og anvendelig. Den skal kunne auditeres og anvendes aktivt i ledelsesrapportering og prioritering af sikkerhedsindsatser. Den skal også være skalerbar og tilpasset kommunens organisatoriske kompleksitet og tekniske afhængigheder.

2.1 Etablering af risikostyringsramme

Kommunen skal udarbejde og vedtage en politik for risikostyring, som definerer formål, metode, roller og ansvar. Politikken skal være forankret i ledelsen og godkendes af den relevante ledelse, med henvisning til § 7, stk. 1 i NIS2-loven. Den skal afspejle kravene i § 6, stk. 1, nr. 1 og nr. 6, som blandt andet omfatter både risikoanalyse og vurdering af effektiviteten af foranstaltninger. Det anbefales, at der til politikken knyttes en procedure for risikostyring, som beskriver den egentlige proces for risikovurdering, herunder roller og ansvar. Selve risikovurderingen understøtter ledelsens beslutningsgrundlag ved at synliggøre, hvor kommunen er mest sårbar, og hvor der skal sættes ind.

I vejledning til NIS2-loven "vejledning om implementering af cybersikkerheds-foranstaltninger, afsnit 1.B" står angivet hvad politikken bør indeholde.

Det anbefales at politikken er tilgængelig for dem det måtte være relevant for. Det kunne fx være systemejere, systemforvaltere, informations-sikkerhedskoordinatorer mv. Det anbefales der-udover at politikken indgår som en central del af kommunens ISMS eller tilsvarende ledelsessystem.

Nedenfor findes et udkast til indhold i en politik for risikostyring, der tager udgangspunkt i NIS2-kravene. Det anbefales, at der udarbejdes en fælles politik for risikostyring, der omfatter både NIS2, GDPR og principperne i ISO27001, så siloimplementeret risikostyring undgås. Såfremt kommunen allerede har integreret risikostyring i den gældende informations-sikkerhedspolitik, vil det være muligt at indarbejde udvalgte afsnit fra nedenstående udkast i den eksisterende politik. Nedenfor er desuden skabelon til risikostyrings-procedure. De to eksempler kan downloades her.

- Eksempel – Politik for Risikostyring
- Eksempel – Procedure for Risikostyring

2.2 Fælles begreber og værktøjer

For at sikre målbare og ensartede risikovurderinger anbefales det at fastlægge et fælles sæt af begreber og guides, som anvendes på tværs af organisationen. I de følgende afsnit præsenteres nedenstående model.

Disse elementer understøtter en prioriteret, ensartet og effektiv risikostyring, hvor ledelsen får et klart beslutningsgrundlag, og hvor fagområderne kan arbejde struktureret med deres egne risici.

Det anbefales, at den enkelte kommune tilpasser modellen i forhold til egen møde-/rapporteringsintervaller og sammensætning i governance.

Fælles begreber og værktøjer	
Risikovurderingsramme	En konsekvens- og sandsynlighedsskala i en 4x4-model, der danner grundlag for en risikomatrix
Risikomatrice og risikohåndtering	Et overblik over metoder til at vurdere og prioritere risici via risikomatrice samt en struktureret tilgang til håndtering
Frekvens for risikovurderinger	Et overblik over anbefalede frekvenser
Risikovurdering af kritiske systemer og tjenester	Et overblik over trin i risikovurderingsprocessen og dokumentation
Guide til identifikation af kritiske aktiver	Step-by-step guide til identifikation af systemer, infrastruktur og integrationer, hvor risikovurdering skal prioriteres

Figur 2.2.1

2.2.1 Risikovurderingsramme

For at sikre kvalitet og ensartethed i risikovurderingerne
er det essentielt at have en referenceramme. Det anbefales, at man fastlægger en skala for hhv. konsekvens og sandsynlighed, som implementeres på tværs af kommunen til anvendelse i risikovurderinger for cyber- og informationssikkerhed samt databeskyttelse.

Den præsenterede model er en 4x4 model, der går fra lav til meget høj konsekvens og fra usandsynligt til forventet sandsynlighed. Modellen har beskrivelser af de enkelte niveauer for henholdsvis konsekvens og sandsynlighed til støtte for vurderingerne. Det anbefales at den enkelte kommune tilpasser og udbygger beskrivelserne for konsekvens.

Konsekvensskala

Niveau	Konsekvens	*Drift*	*GDPR*	NIS2
1	Lav	*Midlertidig forstyrrelse uden påvirkning af drift*	*Registrerede kan opleve få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats*	• Forstyrrelsen har ingen eller minimal betydning for kommunens væsentlige tjenester. • Ingen borgerrettede funktioner påvirkes, og hændelsen kan håndteres uden eskalering.
2	Medium	*Begrænset nedbrud, hurtig genopretning*	*Registrerede kan opleve betydelige uhensigtsmæssigheder, som de kan overkomme med en indsats og overvindelse af nogle få besværligheder*	• En væsentlig tjeneste oplever kortvarig nedgang i funktionalitet (fx under 4 timer), men der findes nødprocedurer. • Begrænset påvirkning af borgere, og hændelsen kan løses med standardindsats.
3	Høj	*Nedbrud af centrale systemer, påvirkning af service*	*Registrerede kan opleve betydelige konsekvenser, som kun kan overkommes med betydelig indsats og konsekvenser for den enkelte*	• En væsentlig tjeneste er ude af drift i længere tid (fx mere end 4 timer, op til 24 timer). • Betydelig påvirkning af borgere og kommunale processer. • Kræver ekstraordinær indsats og mulig eskalering til ledelsen.
4	Meget høj	*Tab af data, langvarig driftsforstyrrelse*	*Registrerede kan opleve betydelige og indgribende konsekvenser, som det ikke er muligt eller kun vanskeligt muligt at overkomme*	• En eller flere væsentlige tjenester er helt utilgængelige i længere tid (fx over 24 timer). • Kritisk påvirkning af borgernes rettigheder og kommunens lovpligtige opgaver. • Kræver aktivering af beredskabsplan og mulig national rapportering

Figur 2.2.1.1 – Figuren kan tilpasses den enkelte kommune
Det forventes, at kommunerne andetsteds, har taget stilling til konsekvensvurdering af henholdsvis Drift og GDPR, hvorfor denne ikke behandles yderligere her. Obs på at der vil være sammenhæng mellem de tre områder.

Sandsynlighedsskala
Sandsynligheden sættes dels ud fra trusselsniveau og dels ud fra vurdering af egen modstands-dygtighed.

Trusselsniveauet kan vurderes, dels ud fra kendskabet til lignende hændelser og dels ud fra aktuelle vurderinger fra SAMSIK, KommuneCert og evt. fra ENISA.

Modstandsdygtigheden vurderes ud fra egen modenhed i forhold til implementering af passende foranstaltninger. Der kan tages udgangspunkt i de specifikke tekniske NIS2 krav (MFA, adgangsstyring, logning og overvågning, kryptering), evt. "Tekniske Minimumskrav for statslige myndigheder" (SikkerDigital.dk) samt SAMSIK's generelle vejledninger om cybersikkerhed.

For at få en vurdering af sandsynlighed anbefales det derfor at inddrage nøglepersoner fra IT drift/ infrastruktur, sådan at der, ud over system-mæssige sårbarheder, også udarbejdes et retvisende billede af sårbarheder og modstands-dygtighed i forhold til IT-infrastrukturen.

Sandsynlighedsskala

NR	Sandsynlighed	Beskrivelse
1	**Usandsynligt**	Det anses for usandsynligt at hændelsen vil forekomme - Ingen erfaring/kendskab til hændelsen fra egen eller sammenlignelige organisationer - Anbefalede foranstaltninger er implementeret til sikring mod sårbarheder, der er løbende opfølgning, justering og vurdering af, om der skal træffes yderligere foranstaltninger Lovgivning og best practise følges. - Truslen vurderes som lav
2	**Mindre sandsynligt**	Hændelsen forventes ikke at komme - Mindre erfaring med hændelsen - kun kendskab til få andre, ikke helt sammenlignelige, organisationer - Anbefalede foranstaltninger er implementeret til sikring mod sårbarheder - Lovgivning og best practise følges - Truslen vurderes som lav
3	**Sandsynligt**	Det er sandsynligt, at hændelsen vil forekomme - Erfaring med eller kendskab til hændelsen fra egen eller sammenlignelige organisationer Manglende foranstaltninger, så sårbarheder kan udnyttes - Lovgivning og best practise følges kun delvist - Truslen vurderes som høj/middel
4	**Forventet**	Det kan forventes, at hændelsen vil forekomme - Erfaring med eller kendskab til hændelsen fra egen eller sammenlignelige organisationer - Manglende foranstaltninger, så mange og åbenlyse sårbarheder kan udnyttes - Lovgivning og best practise følges ikke, - Truslen vurderes som høj, meget høj

Figur 2.2.1.2 – Figuren kan tilpasses den enkelte kommune

2.2.2 Risikomatrice og risikohåndtering

Jf. "Sektorspecifik NIS2 vejledning til kommuner" skal kommunen implementere foranstaltninger ud fra en risikobaseret tilgang. Det anbefales derudover at kommunen fastsætter niveau for risikoaccept, se yderligere i afsnit 1.1 Etablering af governancemodel.

Med udgangspunkt i de foreslåede konsekvens- og sandsynlighedsniveauer defineres risikomatricen som følger:

Risikomatrice

Konsekvens					
	Meget høj	4	8	12	16
	Høj	3	6	9	12
	Medium	2	4	6	8
	Lav	1	2	3	4
		Usandsynligt	Mindre sandsynligt	Sandsynligt	Forventet
		Sandsynlighed			

Figur 2.2.2.1 – Figuren kan tilpasses den enkelte kommune

Risikoaccepten forklarer, hvilket risikoniveau kommunen som udgangspunkt accepterer. Det er op til ledelsen at beslutte, hvornår en risiko er grøn (og dermed accepteres) og det skal klart fremgå af risikomatricen.

Med farveinddelingerne i risikomatricen og det tilhørende skema præciseres de afledte handlinger på de forskellige niveauer.

Nedenstående metodik og skema er udarbejdet på baggrund af best practise. Indholdet i skemaet skal ses som et eksempel, som den enkelte kommune selv kan tilpasse.

Risikohåndtering

Risikoniveau	Tidsramme for udarbejdelse af handleplan og igangsætning af mitigerende foranstaltninger	Ansvarlig for at godkende og igangsætte mitigerende handlinger for mitigering af risiko	Godkendelse & Ressourcer Sikring af den nødvendige ledelsesgodkendelse og ressourcer til risikohåndtering, hvis det ikke kan løftes indenfor egen afdeling/økonomi	Eskalering Identificerer hvornår og hvordan der bør eskaleres i organisation
Lav	Inden for 3 mdr. (*eller risiko accepteres)*	Systemejer / IT-drift	Ingen formel godkendelse nødvendig. Ressourcer fra eksisterende drift.	Ingen eskalering nødvendig.
Medium	Inden for 1 måned	Systemejer / IT-drift	Godkendelse af afdelingschef. Ressourcer allokeres via driftsbudget ved behov.	Eskalering til ledelsesniveau ved manglende fremdrift.
Høj	Inden for 1 uge	Fagchef / ISU / IT-ledelse	Godkendelse af IT-ledelse Ressourcer prioriteres via ledelsesmæssig beslutning.	Eskalering til direktion ved kompleksitet eller afhængighed.
Kritisk	Indenfor 24-48 timer	Fagchef / ISU / IT-ledelse	Godkendelse af IT-ledelse + evt. direktion. Ekstraordinær ressourceallokering.	Eskalering til kommunaldirektør og evt. politisk niveau. Inddragelse af beredskab og eksterne myndigheder.

Figur 2.2.2.2 - Skemaet kan tilpasses den enkelte kommune.

Det skal understreges at det ikke altid er muligt at mitigere en given risiko. Af den grund er det muligt - udover mitigering - at acceptere, overføre eller undgå. Ens for alle handlinger er, at godkendelse skal følge den til en hver tid gældende politik og procedure for risikostyring.

2.2.3 Frekvens for risikovurderinger

Risikovurderinger skal gennemføres regelmæssigt og opdateres ved væsentlige ændringer i trusselsbilledet, teknologi eller organisering. Som udgangspunkt anbefales det at alle kritiske systemer og processer vurderes mindst én gang årligt, men følgende situationer kræver særskilt opfølgning:

- Ved større ændringer, f.eks. ny leverandør, væsentlige systemopdateringer eller organisatorisk omlægning, skal risikovurderingen opdateres uanset det faste interval.
- Ved hændelser, f.eks. databrud, nedbrud eller cyberangreb, skal risikovurderingen revideres straks og danne grundlag for eventuelle korrigerende tiltag.
- Ved høj rest-risiko skal vurderingen eskaleres til ledelsen og kan medføre yderligere analyse
- Ved lav risiko kan vurderingen indgå i den årlige ledelsesgennemgang og dokumenteres som uændret, forudsat at der ikke er sket væsentlige ændringer.

Denne tilgang sikrer, at risikostyringen er både dynamisk og dokumenterbar.

Herunder er eksempel på hvordan man kan skabe overblik og beslutte, hvor ofte aktiver skal genvurderes ud fra kritikalitet og samtidig dokumentere hvem, der er ansvarlig og hvilke vurderinger, der kræver godkendelse på andet niveau end hos den udførende. Den enkelte kommune kan selv justere i dette.

Frekvens

Kritikalitet	Eksempler	Anbefalet hyppighed	Ansvarlig	Godkendelse	Eskalering
Lav	Systemer med begrænset forretningsmæssig betydning (og ikke vurderet som NIS2 kritisk). Behandler ingen personoplysninger.	Hvert 3. år eller ved større ændringer eller større hændelser	Systemejer / IT-drift	Ingen formel godkendelse	Ingen
Medium	Systemer med betydning for servicekvalitet, men med mindre kritisk NIS2 betydning. Behandler muligvis almindelige personoplysninger.	Hvert 2. år eller ved ændringer i system, leverandør eller trusselsbillede eller ved større hændelser	Informationssikker-hedskoordinator	Fagchef / afdelingsleder	Ved manglende opfølgning
Høj	Systemer med betydning for borgervelfærd helbred, rettigheder, økonomi eller lovpligtige opgaver. Behandler sandsynligvis følsomme personoplysninger	Min. hvert år og ved relevante hændelser eller ved ændringer i system, leverandør eller trusselsbillede.	Fagchef / serviceejer / systemejer	Direktørniveau	Ved manglende mitigering eller høj rest-risiko
Kritisk	Systemer der understøtter livsvigtige funktioner fx kritiske tjenester jf. NIS2, såsom beredskab, pleje, forsyning.Behandler sandsynligvis følsomme personoplysninger	Min hvert år straks ved hændelser eller ændringer i system, leverandør eller trusselsbillede	Direktion / serviceejer / systemejer / beredskabsledelse	Direktionen	Politisk niveau / eksterne myndigheder

Figur 2.2.3.1 - Skemaet kan tilpasses den enkelte kommune.

Ud over, at det er væsentligt at have styr på frekvensen af risikovurderinger, er det også vigtigt at have et centralt risiko-register, hvor der løbende er fokus på mitigering og hvor der bliver fulgt op på handleplaner.

2.2.4 Risikovurdering af kritiske systemer og tjenester

Kommunen skal identificere og risikovurdere alle systemer og tjenester, der er væsentlige for opretholdelsen af kommunale kerneopgaver. Det omfatter både tekniske systemer og organisatoriske processer, herunder:

- Fagsystemer med følsomme persondata (fx ESDH, økonomi, sundhed)
- Selvbetjeningsløsninger og borgerportaler
- Infrastruktur til kommunikation, drift og beredskab
- Integrationer og afhængigheder til eksterne leverandører og nationale platforme

Dette følger af § 6, stk. 1, nr. 1 i NIS2-loven, som kræver politikker for risikoanalyse og informationssystemsikkerhed, og yderligere præciseres i vejledning om implementering af cybersikkerhedsforanstaltninger afsnit 1.B.

Det anbefales at risikovurderingen gennemføres i følgende trin:

1. Identifikation af kritiske processer og opgaver
2. Identifikation af systemer, der understøtter de kritiske processer
3. Kortlægning af afhængigheder, integrationer og leverandørrelationer
4. Analyse af trusler, sårbarheder og eksponering
5. Vurdering af sandsynlighed og konsekvens
6. Beregning af risikoniveau og residual risiko
7. Prioritering og anbefaling af foranstaltninger

For guide til identifikation at kritiske processer se afsnit 2.3

Dokumentation og sporbarhed
Det anbefales at alle risikovurderinger dokumenteres med:

- Dato, system, ansvarlig og metode
- Identificerede risici og vurderingsresultater
- Anbefalede foranstaltninger og godkendelsesstatus
- Link til relevante politikker, procedurer og beredskabsplaner

Dokumentationen skal være sporbar og kunne anvendes ved audit, tilsyn og ledelses-rapportering. Den kan opbevares i kommunens ISMS eller tilsvarende styringssystem og være tilgængelig for relevante aktører. Alle risikovurderinger skal revurderes jf. den passende afsnit 2.2.3 "Frekvens for risikovurderinger".

2.2.5 Risiko-scenarier

NIS2-loven tager udgangspunkt i en risikostyring, der omfatter alle farer (all-hazards approach). Det betyder, at kommunen i princippet skal tage højde for alle de trusler, den står overfor, og alle de sårbarheder, den har. Det kan være tekniske og menneskelige fejl, miljømæssige påvirkninger (eksempelvis skybrud m.v.) og direkte bevidste handlinger (f.eks. cyberangreb). For yderligere input, se KL's Drejebog for Informationssikkerhed.

For at gøre risikoarbejdet mere konkret og tilgængeligt anbefales det at vedligeholde et register over relevante risikoscenarier, som kan anvendes, når systemansvarlige m.v. skal klædes på – og konkret udføre risikovurderinger. Scenarierne hjælper til at gøre risikoarbejdet mere virkelighedsnært, idet de oversætter trusler til forståelige beskrivelser af, hvad der kan ske. Ud fra scenarierne er det nemmere at analysere og diskutere, hvilke konsekvenser det kan få for kommunen og hvor sandsynligt det er, ud fra de sårbarheder, der kan udnyttes.

Udover at tage udgangspunkt i trussels-vurderingerne fra SAMSIK er der udarbejdet 5 risikoscenarier som hjælp. De findes ved bilag 1b: Risiko-scenarier.

Det er vigtigt løbende at vurdere risikoscenarierne i forhold til om de stadig er relevante og om der skal tilføjes nye risikoscenarier.

2.3 Identifikation af kritiske processer, systemer og tjenester

Jf. Vejledning til kommuner om NIS2-loven skal kommunen implementere de foranstaltninger (tekniske, operationelle og organisatoriske), der vurderes nødvendige for at opnå et passende niveau af sikkerhed i forhold til levering af den eller de ydelser, som gør, at enheden er omfattet af NIS 2-loven. Samtidig bør vurderingen, og de efterfølgende risikomitigerende tiltag, prioriteres først på de mest kritiske aktiver, dog med hensyntagen til at alle kritiske aktiver skal gennemgås.

Nedenstående step-by-step guide skal give kommunerne en struktureret tilgang til kort-lægning og identifikation af kritiske processer samt tilhørende systemer og integrationer. Aktiver som der efterfølgende skal udføres risiko-vurderinger af.

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"

Figur 2.3.1

Figuren viser en anbefalet guide til at identificere kritiske processer som understøtter kommunale opgaver. Hvert trin i guiden er koblet sammen med tre centrale fokusområder: kortlægning, risikostyring, leverandør-styring og hændelseshåndtering.

Det betyder:
- Fra trin 1 til 2 skal de kritiske opgaver og processer kortlægges
- Fra trin 3 til 6 skal de identificerede aktiver risikovurderes.
- Fra trin 4 til 6 skal der også tages højde for leverandørstyring og hændelseshåndtering.

Guiden findes her: Guide til identifikation af kritiske processer, understøttende systemer, infrastruktur og integrationer og herunder følger en kort gennemgang af guidens anvendelse. Nummereringen henviser til særskilte trin i metoden:

1. Kommunen starter med at vælge et opgaveområde fra en prædefineret liste, fx baseret på Finansministeriets oversigt over kommunens opgaver eller på KLE. Se evt. også casen fra Aarhus Kommune: Aarhus case. Det antages her, at Kommunen har et forudgående kendskab til, hvilke områder, der er mest kritiske for deres drift. Kommunen bør gennemgå alle opgaver for at få et komplet overblik, men rækkefølgen bestemmer kommunen selv.

2. Med baggrund i den valgte opgave, identificeres og kortlægges alle understøttende processer.

3. De kritiske processer identificeres og udvælges. I fase 3 "Identifikation af kritiske processer" findes hjælpespørgsmål til dette.

4. Kommunen udvælger én af de identificerede kritiske processer, og kortlægger de systemer, der understøtter den. I Fase 4 – Identifikation af systemer findes hjælpespørgsmål til dette. Det anbefales at inddrage den fagansvarlige del af organisationen.

5. Kommunen identificerer de underliggende infrastrukturkomponenter til de understøttende systemer. I Fase 5 – Identifikation af infrastrukturelle komponenter findes hjælpespørgsmål til dette. Her bør IT/netværksafdelingen inddrages for at sikre en fuld kortlægning.

6. Kommunen kortlægger de relevante integrationer. Det er vigtigt at skelne mellem tre typer (a, b, c):

a. Interne integrationer
Integrationer mellem systemer, som kommunen selv har fuld kontrol over. Det betyder, at kommunen har ansvar for både drift, vedligeholdelse og sikkerhed.

b. Eksterne integrationer
Integrationer til systemer uden for kommunens kontrol – fx nationale løsninger som FMK (Fælles Medicinkort) eller CPR-registeret.

Det er vigtigt at være opmærksom på eventuelle afhængigheder og risici, da kommunen ikke har indflydelse på den eksterne parts drift, tilgængelighed eller support. For at få problemstillingen løst, skal der rettes henvendelse til den relevante eksterne aktør, som har ansvaret for det pågældende system

c. Semi-eksterne
Semieksterne integrationer til systemer, hvor kommunen har delvis indflydelse, f.eks. gennem medlemskab, governancestruktur eller fælles drift, men ikke har fuld kontrol over teknisk drift, udvikling eller support. F.eks.: KOMBIT-løsninger som KY, KSD, SAPA
Karakteristika:

- Kommunen har typisk medbestemmelse via styregrupper, brugerfora eller kontraktlige aftaler
- Drift og udvikling varetages af ekstern leverandør
- Support og tilgængelighed er ikke direkte styret af kommunen, men der er etableret kontaktveje og eskaleringsmekanismer
- Risici vurderes både ud fra teknisk afhængighed og governance-kompleksitet

I Fase 6 – Identifikation af kritiske integrationer findes hjælpespørgsmål til dette.
Det anbefales at inddrage IT- og netværksafdelingen for at sikre en fuldstændig kortlægning af integrationerne og deres betydning for de kritiske processer.

Når kommunen har gennemarbejdet den valgte kritiske proces, gentages processen for den næste kritiske proces, indtil alle kritiske processer er kortlagt. Det anbefales løbende at genbesøge vurderingen for sikring af at kortlægningen er opdateret i henhold til nye/ændrede processer, systemer mv.

2.4 Ledelsesrapportering

Ledelsesrapportering af risici er en central del af kommunens styring af cyber- og informationssikkerhed. Den sikrer, at ledelsen har et opdateret og beslutnings-relevant overblik over de væsentligste trusler, sårbar-heder, risici og residuale risici der kan påvirke kommunens evne til at levere kritiske tjenester og beskytte borgernes data.

Rapporteringen understøtter ledelsens ansvar for at prioritere ressourcer, godkende risikohåndtering og sikre efterlevelse af NIS2. Den sikrer transparens, og skaber sporbarhed og mulighed for rettidig opfølgning. Dertil bidrager en god ledelsesrapportering til at modne organisationens sikkerhedskultur.

Kvartalsvis rapportering anbefales, for at sikre, at risikobilledet følges løbende, og at væsentlige ændringer, herunder ved nye leverandører, systemopdateringer, organisatoriske omlægninger eller hændelser, bliver adresseret og dokumenteret. Ved høj residual risiko skal ledelsen involveres og vurdere behovet for yderligere tiltag. Ved lav risiko kan status dokumenteres som uændret og indgå i den årlige ledelsesgennemgang.

Risikorapportering sker i sammenhæng med generel ledelsesrapportering: ISU - rapportering til Direktionen. Download den på Videncenteret her.

Bilag 1a: Oversigt over centrale krav til risikostyring

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. 1	Enheden skal have en politik for risikoanalyse.	Skal	Organisationen skal udarbejde og vedligeholde en formel politik for styring af cybersikkerhedsrisici
§ 7, stk. 1	Foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, og regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan	Skal	Risikobehandlingsstrategier og -foranstaltninger skal godkendes og dokumenteres
§ 7, stk. 2	Enheden skal deltage i relevante kurser om cybersikkerhed og risikostyring	Skal	Kompetenceopbygning i risikovurdering og -styring er påkrævet.
§ 7, stk. 3	Enheden bør tilskynde til uddannelse af medarbejdere i cybersikkerhed.	Bør	Organisationen bør fremme risikobevidsthed og træning i risikohåndtering.

Centrale krav til risikostyring i NIS2-direktivet

Artikel	Krav	Kravstype	Indhold
Artikel 20, stk. 1	Ledelsesorganet i enheden skal godkende foranstaltninger til håndtering af cybersikkerhedsrisici og overvåge deres gennemførelse.	Skal	Strategisk og operationelt ansvar placeres direkte hos ledelsen.
Artikel 20, stk. 2	Medlemmer af ledelsesorganet skal have tilstrækkelig viden og kompetence til at vurdere cybersikkerhedsrisici og konsekvenser.	Skal	Krav om kompetenceopbygning og organisatorisk kapacitet i ledelsen.
Artikel 21, stk. 1	Enheden skal godkende og overvåge foranstaltninger til håndtering af cybersikkerhedsrisici.	Skal	Risikostyring skal afspejle trusselsniveau, entitetens størrelse og eksponering, og sikre passende sikkerhedsniveau
Artikel 21, stk. 2, a)	Enheden skal have politikker for risikoanalyse og informationssikkerhed.	Skal	Formaliseret tilgang til risikovurdering og sikkerhedspolitik.

Centrale vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIK's Vejledning til Implementering af Cybersikkerhedsforanstalt-ninger	Enheden skal udarbejde en politik for risikostyring	Skal	Politikken skal indeholde metoder til at identificere og adressere relevante risici i net- og informationssystemer

Bilag 1b: Risiko-scenarier

Introduktion
Risiko-scenarierne kan benyttes i risikovurderingen, fordi det ofte er en hjælp at have noget konkret, nærværende og realistisk at forholde sig til. I kan frit tilpasse scenarierne, så de giver mest mulig mening for jer. Ligeledes kan I frit udvide med flere scenarier end de 5 eksempler, der præsenteres her.

Sådan bruges scenarierne:

Konsekvensvurdering:
Med udgangspunkt i scenarierne vurderer I de mulige konsekvenser for kommunens kritiske opgaver/services. Her skal I betragte scenarierne, som noget, der allerede er indtruffet.

I taler de mulige og konkrete konsekvenser igennem og benytter jeres konsekvens-skala til indplacering af konsekvensniveau.

Sandsynlighedsvurdering:
Med udgangspunkt i scenarierne afdækker I, hvordan hvert scenarie kan udspille sig og hvilke sårbarheder, der vil kunne udnyttes. I gennemgår samtidig jeres eksisterende foranstaltninger og vurderer hvor godt de beskytter jer. Dette skal ses i sammenhæng med det aktuelle trusselsniveau og indsigt i udviklingen i angrebsmetoder m.v. I benytter jeres sandsynligheds-skala til indplacering af sandsynlighed.

Scenarie 1 - Kompromittering af brugeroplysninger via phishing

Hændelsesforløb
En medarbejder falder for et phishing-angreb, hvilket giver en trusselsaktør adgang til interne systemer. Angriberen eskalerer privilegier og får adgang til følsomme data og driftskritiske systemer.

Overvejelser til vurdering af konsekvens
- Hvilke systemer og data kan kompromitteres?
- Hvilken påvirkning vil det have på kerneopgaver og servicelevering[1]
- Er der risiko for kompromittering af systemer eller data, der understøtter essentielle tjenester, med potentielle konsekvenser for fortrolighed, integritet, tilgængelighed og driftskontinuitet

Overvejelser til vurdering af sandsynlighed
- Hvor ofte oplever vi phishing-forsøg?
- Har vi haft tidligere hændelser med succesfulde phishing-angreb?
- Hvor effektiv er vores awareness-træning og tekniske filtrering?
- Brug gerne SAMSIK's trusselsvurdering vedr. phishing-mails

[1]Som afdækket i "Guide til identifikation af kritiske processer, understøttende systemer, infrastruktur og integrationer"

Scenarie 2 - Uvarslet strømsvigt i hele kommunen

Hændelsesforløb
Et omfattende strømsvigt rammer hele kommunen, hvilket medfører nedlukning af servere, netværk, telefoni og fagsystemer. Backup og redundans kan være begrænset.

Overvejelser til vurdering af konsekvens
- Hvor længe kan kerneopgaver opretholdes uden IT-understøttelse?
- Er der nødstrømsløsninger til kritiske systemer?
- Hvilke borgere eller tjenester bliver mest påvirket?

Overvejelser til vurdering af sandsynlighed
- Hvor ofte har vi oplevet strømafbrydelser i kommunen?
- Har vi redundans eller nødstrømsanlæg?
- Er der kendte risici i lokal infrastruktur (fx gamle elnet)?

Scenarie 3 - Ransomware-angreb på kritiske systemer

Hændelsesforløb
En ransomware-inficering krypterer data i fagsystemer og driftskritiske systemer. Angriberen kræver løsesum for at gendanne adgangen. Backup kan ligeledes være kompromitteret.

Overvejelser til vurdering af konsekvens
- Hvor hurtigt data og systemer gendannes uden at betale løsesum?
- Hvilke konsekvenser har det for services til borgere og lovpligtige opgaver?
- Er der risiko for at angriberen lækker data?

Overvejelser til vurdering af sandsynlighed
- Har vi tidligere oplevet malware eller ransomware-forsøg?
- Hvor opdaterede er vores systemer og antivirus?
- Har vi segmentering og backup-test?
- Se aktuelle trusselsvurderinger på SAMSIK.dk

Scenarie 4 – Leverandørbrud i forsyningskæden

Hændelsesforløb
En kritisk IT-leverandør oplever et sikkerhedsbrud, som påvirker kommunens adgang til cloud-tjenester eller driftssystemer.

Overvejelser til vurdering af konsekvens
- Hvilke afhængigheder har vi til leverandøren?
- Er der alternative løsninger eller kontraktuelle krav til beredskab (fx krav til beredskabs- og genopretningsplan)[1]?
- Hvordan påvirkes tilgængelighed og dataintegritet?

Overvejelser til vurdering af sandsynlighed
- Hvor kritisk er leverandøren for vores drift?
- Har leverandøren tidligere haft sikkerhedshændelser?
- Har vi indblik i leverandørens sikkerhedsniveau og compliance?

Scenarie 5 – Insidertrussel fra utilfreds medarbejder

Hændelsesforløb
En medarbejder med adgang til kritiske systemer misbruger sine rettigheder til at slette eller ændre data, fx som følge af utilfredshed eller opsigelse.

Overvejelser til vurdering af konsekvens
- Hvilke systemer kan påvirkes af insideradfærd?
- Er der overvågning og logging, der kan opdage misbrug?
- Hvilken skade kan ske, før hændelsen opdages?

Overvejelser til vurdering af sandsynlighed
- Har vi haft tidligere hændelser med insidertrusler?
- Hvor mange medarbejdere har høje privilegier?
- Har vi processer for offboarding og adgangsstyring?