NIS2-koncepter til kommunal implementering

Ledelsesansvar

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 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 Ledelsesansvar
I dette kapitel af den kommunale NIS2-drejebog præsenteres en tilgang til forankring af ledelsesansvar i kommunerne. Ledelsesansvaret for gennemførelse og efterlevelse af NIS2-krav er et bærende element i NIS2-implementering bl.a. ift. at træffe beslutninger om passende foranstaltninger på baggrund af kommunens NIS2-risikovurdering (jf. kapitel 2) samt ift. opfølgning herpå.

Kommunerne kan allerede have etableret en sikkerheds-governance og have fordelt ansvar og opgaver ifm. eksisterende sikkerhedsarbejde med GDPR og informationssikkerhed. Med NIS2 kommer nye krav både til foranstaltninger inkl. processer. Alle kommuner kan dermed have behov for at gennemgå deres nuværende struktur i lyset af NIS2.

Drejebogsmaterialet giver struktur og metode til hvordan man som kommune kan gå til den nødvendige ledelsesforankring. 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

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.

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.

1. Ledelsens ansvar under NIS2

Jf. NIS2-loven § 3, nr. 20 c, har kommunens øverste administrative ledelse det formelle ansvar for styring af cybersikkerhed. Det betyder, at kommunernes ledelsesorgan vil være direktionen eller tilsvarende (SAMSIKs vejledning: Ledelsens rolle og opgaver).

Med ikrafttrædelsen af NIS2-loven står kommunernes direktion over for et skærpet og eksplicit ansvar for cybersikkerhed. Lovgivningen i NIS2-direktivet art. 20-21 stiller ikke blot krav om tekniske foranstaltninger, men placerer det strategiske og operationelle ansvar direkte hos direktionen. Den kommunale topledelse har dermed det centrale ansvar for at sætte retning, skabe rammer og sikre, at sikkerhedsarbejdet er integreret i den samlede styring af kommunen. For at sikre dette anbefales der metodisk systematik, prioritering og tydelig forankring i hele organisationen.

For implementering og efterlevelse af kravene til ledelsesansvaret anbefales det, at kommunerne etablerer en governancestruktur, hvor cybersikkerhed integreres i eksisterende styringsmodeller, beslutningsfora og rapporteringslinjer. Dette er i tråd med NIS2-direktivets artikel 20, stk. 1, som understreger ledelsens ansvar for strategisk forankring og løbende tilsyn.

Direktionens ansvar for cybersikkerhed forudsætter en struktureret og dokumenterbar tilgang til risikostyring, hændelseshåndtering og løbende opfølgning. Det anbefales at direktionen kan redegøre for prioriteringer, fremdrift og beslutninger, der har indflydelse på sikkerhedsniveauet ikke blot som enkeltstående tiltag, men som en integreret del af den kommunale styring.

Ledelsens opgaver og ansvar

Ifølge § 7, stk. 1 i NIS2-loven og artikel 20, stk. 1 i NIS2-direktivet skal direktionen godkende foranstaltninger til håndtering af cybersikkerhedsrisici og overvåge deres gennemførelse. I praksis betyder det, at direktionen skal være involveret i både beslutninger, prioriteringer og opfølgning. Direktionen skal ikke blot godkende strategier og politikker, den skal aktivt stille sig i spidsen for sikkerhedsarbejdet

Derudover fremgår det af § 7, stk. 2 i loven og artikel 20, stk. 2 i NIS2-direktivet, at medlemmer af ledelsesorganet skal have tilstrækkelig viden og kompetencer til at vurdere cybersikkerhedsrisici og konsekvenser. Dette kan opnås gennem en målrettet indsats for kompetenceopbygning og organisatorisk kapacitet. I praksis betyder det, at direktionen skal klædes på til at kunne varetage deres rolle og ansvar under NIS2-loven.

Ifølge SAMSIK's vejledning om ledelsens rolle og opgaver kan direktionen i en kommune udpege en eller flere direktører til at løfte ansvaret i praksis, men direktionen drages kollektivt til ansvar, hvis kommunen ikke efterlever kravene. Hvis ansvaret placeres hos en enkelt direktør, anbefales det at vurdere sårbarheder og afhængighed ift. dennes tilgængelighed ved f.eks. sygdom eller jobskifte, og om direktionen, som helhed, har kompetencer til i tilstrækkelig grad at prioritere cybersikkerhed.

Implementeringsproces for NIS2-lovens krav: ledelsesansvar – styring, roller og dokumentation

Fastlæg roller, ansvar og mandat

Beskriv direktionens ansvar og mandat (strategisk beslutningskompetence, godkendelse af foranstaltninger, tilsynsansvar)

Udvid Informationssikker-hedsudvalg eller udpeg cybersikkerhedsudvalg med repræsentanter fra ledelsen, herunder direktionen

Dokumentér rollefordeling og ansvar

Definér opgaver og styringsstruktur

Kortlæg konkrete opgaver: risikovurdering, godkendelse af sikkerhedsforanstaltninger, tilsyn, rapportering

Etabler governance-struktur: mødefrekvens, rapporteringsformater, beslutningsgange

Integrér krav til kompetencer og uddannelse – både for ledelsen og øvrige ansatte

Trin 1 og 2 er fokus for dette afsnit

Implementér NIS2-krav i praksis

Operationalisér §6-kravene: tekniske, operationelle og organisatoriske sikkerhedsforanstaltninger

Sikre ledelsens godkendelse og dokumentér beslutningsgrundlag

Etabler intern revision eller ekstern auditspor for governance og ledelsestilsyn

Udarbejd ledelsesrapporter med nøgletal, status og anbefalinger

Sikre kontinuitet og løbende forbedring

Implementér governance-loop: opfølgning, justering, læring

Etabler politik eller retningslinjer for uddannelse og awareness (jf. NIS2-loven §6, stk. 1, nr. 7 og §7, stk. 2)

Integrér governance i beredskabsplaner og kontinuitetsstyring

Dokumentér og evaluer governance-effekten årligt

1.1 Etablering af governancemodel

En sammenhængende sikkerhedsindsats
For at sikre en effektiv, sammenhængende og dokumenterbar styring af kommunens arbejde anbefales det at indarbejde cybersikkerhed i den eksisterende risikostyring og beslutningsstruktur. Det vil sikre sammenhæng mellem eksisterende indsatser, f.eks. GDPR og Informationssikkerhed, og kravene der følger af NIS2-loven.

Governancestrukturen kan f.eks. omfatte strategisk ledelse, taktisk koordinering og operationel implementering, og være tilpasset kommunens organisatoriske kompleksitet og risikoprofil.

Denne tilgang understøtter, at cybersikkerhed integreres i kommunens overordnede ledelsessystem frem for at blive behandlet som et isoleret teknisk område. Ved at samtænke sikkerhedsområderne skabes organisatorisk robusthed og en sammenhængende styringsmodel, som gør det muligt at dokumentere indsatsen over for både tilsynsmyndigheder og eksterne parter og understøtter effektivisering indenfor sikkerhedsområderne.

ISO/IEC 27001:2023 kan med fordel anvendes som ramme for governance, da standarden tilbyder en genkendelig og gennemprøvet struktur, der kan understøtte NIS2-kravene på tværs af organisatoriske niveauer:

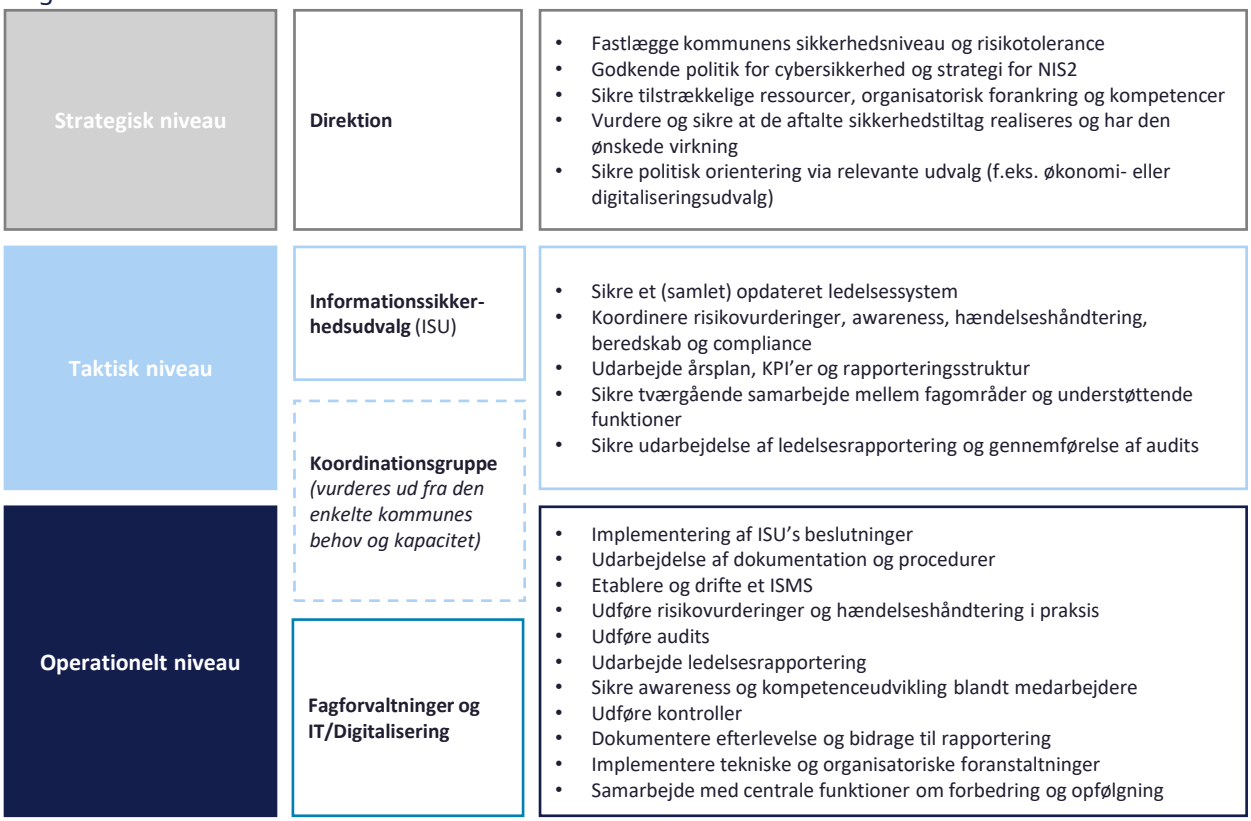
- Strategisk niveau: direktionens ansvar for politik, risikotolerance og ressourcetildeling
- Taktisk niveau: stabsfunktioners rolle i planlægning, koordinering og kontrolmiljø
- Operationelt niveau: teknisk implementering, drift og dokumentation i praksis

Denne flerniveaumodel understøtter en helhedsorienteret tilgang, hvor roller, ansvar og dokumentationskrav er klart defineret og forankret i den samlede styringsstruktur.

De specifikke roller, udvalg og grupper under de tre niveauer skal tilpasses den enkelte kommunes organisering og kapacitet.

Model 2 inkluderer en option for en koordineringsgruppe. Denne gruppe kan dels varetage taktiske og dels operationelle opgaver. Ved mindre kommuner vil det ikke nødvendigvis være fordelagtigt at have både et informationssikkerhedsudvalg (ISU) og en koordineringsgruppe, da pladserne ofte vil være besat af de samme ressourcer i kommunen. Ved større kommuner kan der være behov for flere lag hen over hhv. det taktisk og det operationelle niveau for at sikre passende koordinering mellem forvaltninger.

Find mere information og se eksempler på governancemodeller i bilag 1b-1f.



Model 2

1.2 Ledelsesforankret Cyber- og Informations-sikkerhedsudvalg

Som et godt udgangspunkt for det konkrete arbejde med NIS2-kravene kan kommunerne nedsætte et Cybersikkerhedsudvalg eller udvider det eksisterende Informationssikkerhedsudvalg (ISU) til også at omfatte cybersikkerhed.

Det overordnede ansvar er fortsat forankret ved direktionen, men det er udvalget, der i praksis arbejder med og træffer beslutning om konkretet tiltag og sørger for, at NIS2-kravene implementeres og efterleves i kommunen.

For at kunne udføre de påkrævede opgaver anbefales det, at sikre at udvalget har beslutningskompetence og ledes af en direktionsrepræsentant, der sikrer den nødvendige ledelsesmæssige forankring specificeret i NIS2-loven § 6-7. Hvis udvalget ikke ledes af en direktionsrepræsentant anbefales det, at kommunerne vurderer og dokumenterer, hvordan de kan sikre ledelsesforankringen f.eks. ved at have en fast plads i udvalget til en direktionsrepræsentant, der eventuelt kan variere ud fra deltagerens ansvarsområde eller tilgængelighed. Dertil anbefales det at udvalget sammensættes med tværgående repræsentation, således at udvalget afspejler både teknisk og strategisk ansvar. I praksis betyder det, at udvalget bemandes med repræsentanter fra IT/digitalisering og relevante fagområder ud fra en risikobaseret tilgang tilpasset kommunens organisering.

Eksempler på udvalgets opgaver:

- Koordinere sikkerhedsaktiviteter, herunder sikre gennemførsel af risikovurderinger
- Opfølgning på implementering af politikker og retningslinjer
- Udarbejde årsplaner og fastsætte mål
- Følge op på effekt og rapportere til ledelsen
- Under NIS2 implementeringen bør de desuden løbende sikre den fornødne fremdrift

Der hvor det giver organisatorisk værdi, anbefales det, at kommunerne nedsætter en koordineringsgruppe (som angivet i model 2). Koordineringsgruppen kan med fordel varetage en række taktiske og operationelle opgaver. Det vil sikre, at de ledelsesmæssige lag kan fastholde sit fokus på strategiske og taktiske beslutninger og overlade opfølgning, vurdering og operationelle beslutninger til udvalget.

Anbefalet sammensætning af ISU

ISU rolle	Org. rolle (eksempler)	Funktion i ISU
Formand	Kommunaldirektør eller direktionsrepræsentant	Sikrer ledelsesforankring og rapportering til direktionen
IT/digitalisering	IT og digitaliseringschefer	Bidrager med teknisk indsigt og hændelseshåndtering
Databeskyttelse	DPO/databeskyttelseskoordinator	Rådgiver og understøtter organisationen med at efterleve Databeskyttelsesforordningen (GDPR)
Informationssikkerhed	Informationssikkerhedskoordinator/CISO	Ansvarlig for udvikling og drift af Ledelsessystem for Informationssikkerhed samt koordinering af sikkerhedsindsatsen/NIS2 indsatsen og sikre sammenhæng og synergi i informationssikkerhedsarbejdet (NIS2, GDPR)
Ansvarlige for forretningsunderstøttelse	Chefer med system eller procesmæssigt ejerskab	De roller der ejer risici i forbindelse med systemer og processer skal sikre forretningsforankring og lokal implementering. Beror på hvordan de enkelte forvaltninger skal repræsenteres.
HR/Kommunikation	HR og kommunikationschefer	Understøtter awareness og kompetenceudvikling
ISU-mødeleder	Direktør eller rolle med chefansvar	Leder møderne i ISU, sikrer støtte til udvalgets medlemmer f.eks. Gennem rådgivning
ISU-koordinator	Informationssikkerhedskoordinator eller anden koordinerende rolle	Koordinerer møderne, udarbejder dagsordener, fremsender materiale, sikrer dokumentation fra møderne inkl. referat
Juridisk ansvarlig	Chef for juridisk afdeling eller jurist	Sikrer de interne juridiske afklaringer for regler ved politikker og eksterne juridiske spørgsmål
Specialist roller – roller der kan indkaldes til møder enten på fast basis eller ved emner på dagsorden, hvor det er relevant at få deres input		
Beredskabsansvarlig	Ansvarlig for den fysiske sikkerhed	Ansvarlig for fysisk beredskab og understøtter koordinering mellem fysisk, teknisk og organisatorisk beredskab
Fagspecialister	Teamledere	Har indsigt i og operationelt ansvar for specialist områder f.eks. Netværk, Identify and Access management. Understøtter ISU med specialistviden i deres vurderinger.

1.3 Udvalgsstruktur og ledelsesforankring: mandat, mødefrekvens og eskalationsveje

Møder og frekvens

Det anbefales, at der udarbejdes et årshjul for det ledelsesforankrede udvalg/ISU med faste møder, deadlines for eks. risikovurderinger, awareness, audits og rapportering. Det anbefales at udvikle og anvende tilpassede skabeloner til arbejdet, der gør det ensartet og sikrer den nødvendige dokumentation. Se forslag til følgende skabeloner her:

- ISU-mødeagenda
- ISU-mødereferat
- ISU - rapportering til Direktionen
- ISU-årshjul

Kommunerne kan med fordel følge anbefalingerne i KL's vejledning: Informationssikkerhedsudvalgets organisering. Heri anbefales det, at afholdelse af møder falder ind i en eksisterende møderække, hvor deltagerne i ISU mødes i anden sammenhæng.

Ved fastsættelse af mødefrekvens anbefales det, at der skelnes mellem implementerings- og driftsfase samt ad hoc møder ved eksempelvis hændelser. Særligt ved implementering og ad hoc møder ved hændelser kan der være andre behov, der taler for en anden mødefrekvens.

Mødefrekvens-anbefalinger:

1. Implementering af NIS2:
   - Anbefalet: Hver 1-3 måned. Frekvensen og sammensætningen af udvalget beror på en vurdering, men det anbefales, at en gruppe eller hele udvalget mødes ofte for at fastholde momentum og sikre fremdrift - se foreslåede koordinationsgruppe i model 2.
   - Fokus på fremdrift, beslutninger og dokumentation.
2. Drift og vedligehold:
   - Anbefalet: hvert kvartal.
   - Evaluering, opfølgning og planlægning af forbedringer.
3. Ad hoc:
   - I beredskabsplanen og plan for hændelseshåndtering bør det identificeres, hvordan ISU indkaldes til ad hoc møder for håndtering af og støtte til håndtering af hændelser.

Kommissorium og mandat

Det anbefales, at udvalget har et formelt kommissorium, godkendt af direktionen, som definerer:
- Formål og ansvarsområder
- Sammensætning og mødefrekvens
- Beslutningskompetencer og rapporteringslinjer
- Samspil med koordinationsgruppe og øvrige fora
- Krav til dokumentation og opfølgning

Kommissoriet kan være en udvidelse af et eksisterende kommissorium (for ISU).

Yderligere viden om anbefalinger til ISU samt skabelon til kommissorium kan hentes i KL's Videncenter

Det anbefales, at fastlægge udvalgets mandat til at:
- Godkende og prioritere sikkerhedsaktiviteter og forbedringstiltag
- Godkende risikovurderinger og opfølgning på hændelser
- Vedtage politikker og procedurer inden for ISMS
- Allokere ressourcer inden for rammer fastlagt af direktionen
- Eskalere kritiske risici og hændelser til direktionen
- Godkende it-beredskabsplaner og eskalationsveje

Beslutninger dokumenteres og kan indgå som en del af compliance arbejdets sporbarhed og governance.

Det anbefales, at fastlægge en klar model for eskalering:
- Operationelle hændelser håndteres af CISO/Informationssikkerhedskoordinator og IT, med rapportering til ISU.
- Kritiske risici eller hændelser (fx brud på forsyningskædesikkerhed, brud på persondatasikkerheden, systemnedbrud, trusler mod forsyning) eskaleres til direktionen.
- Strategiske beslutninger (fx ændring af sikkerhedsniveau, investeringer, ændringer i governance) behandles af ISU og godkendes af direktionen

Eskalering skal ske hurtigt og dokumenteret, med tydelige kriterier og ansvar.

1.4 Roller og kompetencer

Det er afgørende, at alle nøglepersoner i kommunen har de rette kompetencer til at varetage deres ansvar. Uden den nødvendige viden og forståelse risikerer kommunen at overse væsentlige trusler eller sikkerhedsbrud, træffe forkerte prioriteringer eller undlade at dokumentere kritiske beslutninger.

Ifølge NIS2-loven § 7, stk. 2 skal direktionen have viden og kompetencer til at styre kommunens cybersikkerheds-risici. Det indebærer, at direktionen selv skal deltage i relevante kurser. Dertil stiller NIS2-loven § 6, stk. 1, nr. 7 og § 7, stk. 2 krav om, at ledelsen tilskynder til uddannelse af relevante medarbejdere, så de besidder den nødvendige viden og de færdigheder, der svarer til deres rolle og ansvar, samt at der tilskyndes til uddannelse af medarbejdere. Direktionen har dermed et direkte ansvar for, at alle centrale funktioner, fra ledelseslag og informationssikkerhedsudvalg til systemejere og driftspersonale, løbende klædes på til at handle korrekt, dokumentere ansvar og bidrage aktivt til en robust og modstandsdygtig sikkerhedskultur.

Anbefalinger til viden og kompetencer:

- **Opbygning af kompetencer** bør ske ved onboarding, rolleændringer eller ved ny NIS2-omfattelse.
- **Vedligeholdelse af kompetencer** kan ske via awareness-træning, e-læring, workshops, netværk eller interne audits.
- **Frekvenserne** er vejledende og bør tilpasses kommunens risikoprofil og organisatoriske kompleksitet.

Model 4 giver anbefalinger til og eksempler på uddannelse og kan integreres i kommunens årshjul for kompetenceudvikling.

Rolle	Eksempler til Kompetenceopbygning	Eksempler til Kompetencevedligeholdelse	Frekvens (vejledende anbefalinger)
Direktion*	Strategisk forståelse af NIS2, ansvar for governance, risikostyring og organisatorisk forankring	Opdatering på lovgivning, tilsynspraksis, trusselsbillede og ledelsesansvar	Opbygning: ved rolleindtræden eller NIS2-omfattelse Vedligeholdelse: 1 gang årligt
ISU-medlemmer	Forståelse af NIS2-rammen, organisatorisk risikostyring, hændelseshåndtering og awareness	Sparring med CISO, opfølgning på compliance gaps og awareness-effekt	Opbygning: ved udpegning til ISU Vedligeholdelse: årligt eller ved større ændringer
Informationssikker-hedskoordinator / CISO *(alt efter hvilken rolle kommunen har)*	Forståelse af NIS2 rammen, Risikovurdering, hændelseshåndtering, leverandørstyring, awareness-programmer	Opfølgning på trusselsbillede, revisioner, awareness-effekt og compliance gaps	Opbygning: ved ansættelse eller rolleændring Vedligeholdelse: månedligt
Systemejer	Risikovurdering, dataklassificering, hændelsesberedskab og leverandørrelationer/styring	Opdatering på systemændringer, trusselsbillede og organisatoriske krav	Opbygning: ved systemtilskrivning Vedligeholdelse: halvårligt eller ved systemændringer
Ansvarlige for forretningsunderstøt-telse (roller med ansvar for taktiske og operationelle opgaver ved processer)	Forståelse af risikostyring, konsekvensanalyse og NIS2's krav til dokumentation og opfølgning	Opdatering på risikoregistre, kontrolmiljø og governance-struktur	Opbygning: ved udpegning som risikoejer Vedligeholdelse: kvartalsvis eller ved audit
Systemadministrato-rer (roller med operationelle opgaver i systemerne)	Risikovurdering, adgangsstyring, patch management, logning, backup og tekniske kontroller	Versionsopdateringer, sårbarhedshåndtering, compliance-tilpasninger	Opbygning: ved onboarding Vedligeholdelse: månedligt eller ved større opdateringer
Operationelle og administrative roller (f.eks. i IT, HR, økonomi, fagforvaltninger)	Awareness, dokumentation, hændelseshåndtering, dataklassificering og -kvalitet, korrekt systembrug, processer og forståelse af sikkerhedskrav	Genopfriskning af awareness, opdatering på arbejdsgange og -processer, vedligeholdelse af kontraktoverblik onboarding-procedure, databeskyttelse og systemfunktioner	Opbygning: ved onboarding Vedligeholdelse: årligt eller ved awareness-kampagner

Model 4

** Den enkelte kommune bør vurdere om det er hele eller dele af direktionen, der skal modtage uddannelse. Det anbefales, at viden og kompetencer ikke udelukkende ligger ved én ressource, da det udgør en sårbarhed i sig selv.*

1.5 Strategisk kommunikation til ledelsen

Hvorfor cybersikkerhed kræver ledelsens opmærksomhed:

I kommunerne er kerneopgaven baseret på, at digitale systemer fungerer sikkert og stabilt. Når hjemmesygeplejen, borgerbetjeningen eller sagsbehandlingen rammes af nedbrud, er det ikke kun IT, der svigter. Det er velfærd, tillid og drift, der står på spil.

Derfor er cybersikkerhed ikke blot et teknisk anliggende, det er et strategisk ledelsesansvar. Direktionen sætter rammerne for risikoprofil, investeringer og prioriteringer. Kun når cybersikkerhed kommunikeres klart, konkret og i øjenhøjde med ledelsen, kan der sikres den nødvendige forankring og fremdrift.

De 10 strategiske greb nedenfor er udviklet til netop dét: at skabe engagement og opbakning fra kommunale ledelser ved at koble cybersikkerhed direkte til kerneopgaven, ansvar og værdi.

Se evt. også casen der er anvendt i en kommune for at skabe forståelse og tilslutning fra medarbejdere og ledelse på vigtigheden af cybersikkerhed: Kommunecasen findes via dette link.

Når vi taler om sikkerhed som en forudsætning for digitalisering og drift, og ikke som en teknisk detalje, får vi ikke bare opmærksomhed. Vi får handling.

10 Strategiske greb til ledelseskommunikation om cybersikkerhed

1. **Kommunikér klart og menneskeligt så alle kan være med**
   Brug almindeligt sprog - drop fagtermer og tekniske forkortelser. Det skal kunne forklares over frokost.
2. **Sæt kerneopgaven i centrum og vis konsekvenserne**
   Forklar hvordan trusler som ransomware direkte påvirker evnen til at løse kerneopgaven. Når data forsvinder, forsvinder også muligheden for at levere.
3. **Gør det konkret med virkelige scenarier**
   Brug eksempler fra hverdagen: Hvad sker der, når hjemmesygeplejen mister adgang til borgerdata og ruter? Det er ikke abstrakt, det er driftstab.
4. **Knyt kommunikationen til det aktuelle trusselsbillede**
   Brug SAMSIK, KommuneCERT og nationale vurderinger som afsæt. Det gør budskabet relevant og rettidigt, og viser, at vi følger med.
5. **Brug eksempler fra aktører med samme udgangspunkt**
   Peg på cases fra lignende organisationer. Det skaber genkendelse og troværdighed, og gør det lettere at oversætte til egen virkelighed.
6. **Digitalisering kræver sikkerhed som fundament**
   Jo mere vi digitaliserer, jo mere sårbare bliver vi. Sikkerhed skal ikke være en bremse men en forudsætning.
7. **Vær ærlig om risikoaccept og konsekvenserne**
   Hvis vi vælger at leve med risici, skal vi også kunne leve med konsekvenserne. Nedbrud koster både i tillid og i drift.
8. **Placér ansvaret dér, hvor beslutningerne kan tages**
   Cybersikkerhed er et ledelsesansvar. Opgaver kan delegeres, men ikke ansvar.
9. **Vis hvad investeringer omsættes til og hvordan de følges op**
   Sæt mål, dokumentér fremdrift og rapportér på udviklingen. Det giver transparens og sikrer, at direktionen får value for money.
10. **Visualisér sikkerhedsniveauet - så alle kan være med**
    Brug visuelle modeller og intuitive indikatorer. Det gør det lettere for ikke-specialister at forstå trusler, indsatser og behov.

Bilag 1a: Oversigt over centrale krav til ledelsesansvar

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 kommunerne, der er identificeret som væsentlige enheder jf. § 2 og § 3 i loven.
Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau (NIS2-direktivet) 2022/2555

Centrale paragraffer i NIS2-loven vedr. ledelsen

§	Krav	Kravstype	Indhold
§ 6, stk. 1, nr. 7	Enheden skal træffe foranstaltninger for uddannelse af relevante medarbejdere.	Skal	Ledelsen skal sikre, at der er cybersikkerhedsuddannelse til relevante medarbejdere.
§ 7, stk. 1	Ledelsesorganet skal godkende foranstaltninger til håndtering af cybersikkerhedsrisici.	Skal	Direktionen har ansvar for godkendelse af sikkerhedsforanstaltninger.
§ 7, stk. 2	Ledelsesorganet skal deltage i relevante kurser om cybersikkerhed og risikostyring.	Skal	Krav om kompetenceopbygning i direktionen.
§ 7, stk. 2	Ledelsesorganet skal tilskynde til uddannelse af medarbejdere.	Bør	Direktionen opfordres til at fremme awareness og træning.

Centrale ledelseskrav 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.

Vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIK's Vejledning om ledelsens rolle og opgaver	Ledelsen bør etablere faste beslutningsfora for cybersikkerhed.	Bør	Governance-struktur med faste møder og rapportering.
SAMSIK's Vejledning om ledelsens rolle og opgaver	(Kommunen) skal have en politik for uddannelse af relevante medarbejdere	Skal	Politikken skal sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende ift. deres rolle og ansvar.
SAMSIK's Vejledning til Implementering af Cybersikkerhedsforanstaltninger	Ledelsen bør sikre, at leverandørstyring inkluderer NIS2-krav.	Bør	Leverandørkontrakter og kontrolmekanismer.

Bilag 1b: Anbefalinger til implementering af governancemodel

Strategisk niveau	Ledelsesopgaven for NIS2-indsatser bør være tydeligt placeret i den øverste administrative ledelse f.eks. hos kommunaldirektøren eller et direktionsmedlem med ansvar for digitalisering og sikkerhed. Cybersikkerhed skal behandles som et strategisk risikoområde og indgå i ledelsens faste risikovurderinger. Tydelig ledelsesforankring sikrer ejerskab og prioritering. Når cybersikkerhed integreres i strategiske risikovurderinger, bliver det en del af kommunens samlede styringsgrundlag og ikke blot et teknisk anliggende. Politisk orientering og beslutning bør ske struktureret og risikobaseret, f.eks. via økonomiudvalg eller relevante ledelsesfora, afhængigt af kravenes karakter og kommunens modenhedsniveau og kapacitet. Størrelsesdifferentiering*:* I større kommuner anbefales fælles ansvar mellem kommunaldirektør og områdedirektører samt politisk orientering via f.eks. Økonomi eller Digitaliseringsudvalg.
Taktisk niveau	Det anbefales, at kommunerne etablere et tværgående sikkerhedsudvalg med mandat til at koordinere og prioritere både NIS2 og ISO27001 aktiviteter. Udvalget bør inkludere relevante funktioner som informationssikkerhedskoordinator, DPO, IT, HR og juridisk rådgivning, og have repræsentation fra direktionen. Dette kan gøres enten gennem en udvidelse af et eksisterende ISU eller ved at nedsætte et nyt udvalg for cybersikkerhed. Et tværgående udvalg sikrer, at beslutninger træffes på et oplyst grundlag, hvor både tekniske, juridiske og organisatoriske hensyn balanceres. Det skaber sammenhæng mellem politikker, awareness, hændelseshåndtering og dokumentation samt reducerer risikoen for silotænkning. Størrelsesdifferentiering*:* I mindre kommuner kan en mindre sikkerhedsgruppe med færre deltagere være tilstrækkelig, mens større kommuner kan supplere med underudvalg i decentrale enheder for at sikre lokal forankring. Ved mellemstore og større kommuner kan det være værdifuldt at nedsætte en koordineringsgruppe der varetager en kombination af taktiske og operationelle beslutninger og opgaver.
Operationelt niveau	Udpeg systemejere og proces- eller områdeejere i relevante fagområder med ansvar for implementering af NIS2-krav, herunder risikovurdering, dokumentation og hændelseshåndtering. IT bør understøtte med tekniske kontroller, drift og operationel håndtering af hændelser. Awareness og kompetenceudvikling bør ske løbende og målrettet. Ved at placere ansvaret tæt på driften sikres ejerskab og praksisnær implementering og håndtering. Det reducerer afhængigheden af centrale funktioner og øger robustheden. En tydelig rollefordeling mellem fagområder og IT skaber klarhed og effektivitet i både forebyggelse og reaktion. Størrelsesdifferentiering*:* Større kommuner kan etablere lokale sikkerhedskoordinatorer og dedikerede IT-sikkerhedsteams (f.eks. SOC), mens mindre kommuner kan samle funktionerne på færre roller f.eks. med støtte fra eksterne leverandører. Dette er i overensstemmelse med SAMSIK's anbefalinger om tilpasning af governance og sikkerhedsstruktur efter organisatorisk kapacitet.
Rapportering	Etabler en fast rapporteringsstruktur med kvartalsvis rapportering til direktion og årlig politisk orientering. Rapporteringen bør inkludere status på risikovurderinger, awareness, compliance og hændelser. Brug datadrevne indikatorer og visuelle oversigter for at understøtte beslutningstagning. Regelmæssig rapportering skaber transparens, fremdrift og mulighed for rettidig justering. Det styrker ledelsens beslutningsgrundlag og dokumenterer efterlevelse af NIS2-krav. En struktureret rapporteringsrytme understøtter også audit og ekstern revision.

Bilag 1c: Implementeringseksempel fra mindre kommune

Strategisk niveau	**Sikkerhedsorganisationen** Direktionen (Sikkerhedsorganisationen) har det overordnede ledelsesansvar for kommunens efterlevelse af NIS2. Sikkerhedsorganisationen fastsætter risikoprincipper og prioriteringer, godkender væsentlige risikoaccepts, tildeler nødvendige ressourcer og følger kvartalsvist op via ledelsesgennemgang med en NIS2-status. Politisk orientering sker årligt via relevante fora eksempelvis økonomiudvalg. Øverste ledelse og relevante chefer gennemfører løbende kompetenceudvikling i cybersikkerhed og NIS2-krav.
Taktisk niveau	**Cybersikkerhedsudvalget** Cybersikkerhedsudvalget (CSU) har mandat til at koordinere og prioritere NIS2- og ISO27001-aktiviteter. CSU rapporterer kvartalsvist til Sikkerhedsorganisationen og består af Chef for IT og Digitalisering, Informationssikkerhedskonsulenten, IT, DPO og 1 medlem af direktionen. Der gennemføres løbende uddannelse for medlemmer af CSU.
Operationelt niveau	**Roller og ansvar på operationelt niveau** Informationssikkerhedsteamet, IT og relevante proces-/systemejere håndterer implementering af NIS2-krav, herunder bl.a. risikovurdering/DPIA, awareness, dokumentation og hændelseshåndtering samt vedligeholdelse af dette. Informationssikkerhedsteamet og IT anvender ISMS/ITSM, som den centrale styringsramme for NIS2-overholdelse. Informationssikkerhedsteamet har ansvaret for den daglige drift af ISMS'et med tilhørende kontroller for hele organisationen. IT har den daglige drift af ITSM samt hændelseshåndtering og dokumentation heraf. Informationssikkerhedsteamet og IT refererer til IT- og Digitaliseringschefen, der fungerer som kommunens SPOC i NIS2-sammenhæng, herunder koordination med kompetente myndigheder/CSIRT og intern eskalation. Indkøbsråd/indkøbsafdeling og proces-/systemejere med ansvar for processer og systemer med høj kritikalitet udpeges og uddannes løbende i overholdelse af NIS2-krav.
Rapportering	Kommunen opretholder en samlet proces for håndtering af hændelser og brud, der kan udløse rapporteringspligt efter GDPR og/eller NIS2. Processen sikrer hurtig klassifikation, koordineret kommunikation, korrekt modtager (Datatilsynet og Styrelsen for Samfundssikkerhed) og overholdelse af gældende tidsfrister. Der føres fælles log og sporbar dokumentation af vurderinger, beslutninger og indsendte rapporter. **Intern rapportering** Informationssikkerhedsteamet udarbejder rapportering, KPI'er og handlingsplaner til CSU og Sikkerhedsorganisationen. Sikkerhedsorganisationen modtager minimum halvårligt en statusrapport om arbejdet med NIS2 og GDPR/Informationssikkerhed fra Cybersikkerhedsudvalget. **Anden rapportering** Kommunen udpeger et internt NIS2-kontaktpunkt (SPOC) placeret i Informationssikkerhedsteamet, der koordinerer kommunikation med kompetent myndighed og nationalt CSIRT samt intern eskalation

Bilag 1d: Implementeringseksempel fra mellemstor kommune

Strategisk niveau	**Direktion og politisk ledelse** Et direktionsmedlem har ansvar for digitalisering og informationssikkerhed. Informationssikkerhed og NIS2 indgår i den årlige strategiske risikovurdering og ledelsesrapportering. Politisk orientering sker via økonomiudvalget til byrådet.
Taktisk niveau	**Integreret informationssikkerhedsudvalg** Udvalget ledes af det ansvarlige direktionsmedlem og består af informationssikkerhedskoordinator, DPO, IT-chef, HR og stabschefer fra fagforvaltningerne. Udvalget har mandat til at koordinere og prioritere både ISO27001 og NIS2-aktiviteter. Udvalget udarbejder en samlet strategi, årsplan og mål for sikkerhedsarbejdet.
Operationelt niveau	**Fagforvaltninger og systemejere** Fagforvaltningerne har ansvar for risikovurdering, hændelseshåndtering og awareness i deres områder. Informationssikkerhedskoordinatorer i forvaltningerne understøtter implementering og dokumentation. IT-afdelingen håndterer tekniske kontroller og beredskab.
Rapportering	**Direktion:** Kvartalsvis rapportering med struktureret status på NIS2-implementering, ISO27001-aktiviteter, risikovurderinger og hændelseshåndtering. Rapportering inkluderer mål, fremdrift og anbefalinger til prioritering. Rapportering sker gennem direktionens deltagelse i ISU. **Kommunalbestyrelse / Økonomiudvalg:** Årlig orientering med fokus på strategisk status, compliance, beredskab og eventuelle større hændelser. Kan kombineres med status på digital infrastruktur og databeskyttelse. **Informationssikkerhedsudvalg:** Mødes kvartalsvis med opfølgning på årshjul, risici, awareness og implementering. Rapportering til den øvrige direktion efter hvert møde og ved væsentlige afvigelser sker gennem det deltagende direktionsmedlem efter behov.

Bilag 1e: Implementeringseksempel fra mellemstor kommune

Strategisk niveau	**Direktion og politisk niveau** Kommunaldirektøren har sammen med direktionen ansvaret for Informationssikkerhed og NIS2. Strategisk ledelsesrapportering 3 gange årligt heraf 1 årsrapport hvor blandt andet risikoaccept gennemgås. Direktionen er ansvarlig for at viderebringe relevant orientering til politisk niveau/økonomiudvalget
Taktisk niveau	**Integreret informations- og cybersikkerhedsudvalg** Udvalget ledes af CISO (delegeret fra kommunaldirektøren til Stabschefen for Personale & Digitalisering). Udvalget består af: Direktionen (samlet), CISO/Stabschef for Personale & Digitalisering, IT-chef, Teamleder for sikkerhedsområdet, DPO (ved behov) Udvalget har mandat til at koordinere og prioritere alle aktiviteter inden for informations- og cybersikkerhed herunder også NIS2-aktiviteter – der udarbejdes en samlet strategi, årsplan og KPI'er for sikkerhedsarbejdet.
Operationelt niveau	**Fagforvaltninger og systemejere** Systemejere har ansvar for risikovurdering, hændelseshåndtering og awareness i deres områder. Lokale kontaktpersoner understøtter implementering og dokumentation. IT-afdelingen håndterer sikkerhedsarbejdet for IT-miljøet, herunder tekniske kontroller, fælles systemer og beredskab. Dertil støtter de systemejere med faglig viden ved indkøb af nye systemer fx ift. datasikkerhed og sikker integration af systemer til IT-miljøet.
Rapportering	**Direktion – sammen med Informations- og cybersikkerhedsudvalgsmøde (ISU)** Rapportering 3 gange årligt med struktureret status ift. NIS2-implementering samt andre relevante standarder (ISO/CIS). Rapporten inkluderer blandt andet: - KPI'er for sikkerhedsniveauet - Gennemgang af fremdrift siden sidste rapport - Risikovurdering - Hændelseshåndtering - Emner til drøftelse ift. ledelsesbeslutning Årlig rapport med fokus på: - Status jf. den strategiske indsats - Drøftelse og beslutning ift. at ændre risikoaccept/indsatsen ift. NIS2 **Koordineringsgruppe for informations- og cybersikkerhed** Månedlige møder med opfølgning på det samlede sikkerhedsarbejde herunder aktuel programplan for cybersikkerhed, Governance og compliance for ISO/GDPR. Viderebringer relevante emner til ISU-møder.

Bilag 1e: Implementeringseksempel fra stor kommune

Strategisk niveau	**Direktion og politisk niveau** Kommunaldirektøren og forvaltningsdirektører har et fælles ansvar for informationssikkerhed og NIS2 i kommunen. Strategisk ledelsesrapportering til dette niveau inkluderer afrapportering og status på sikkerhed, compliance og hændelser. Ved behov kan politisk orientering ske r via relevante udvalg, eksempelvis Økonomiudvalget eller øvrige råd og/eller udvalg.
Taktisk niveau	**Informationssikkerhedsudvalg** Udvalget ledes af en CISO eller digitaliseringschef og består af informationssikkerhedskoordinator, DPO, IT-sikkerhedschef(er), repræsentanter fra alle forvaltninger, HR, jura og beredskab. Underudvalg i hver forvaltning varetager lokal koordinering. Udvalget arbejder med og sikrer strategi, compliance, audit og koordinering af både NIS2 , ISO27001, GDPR og øvrigt sikkerhedsarbejde.
Operationelt niveau	**Decentrale enheder og systemejere** Systemejere og procesejere har ansvar for implementering, risikovurdering og dokumentation. Lokale sikkerhedskoordinatorer sikrer awareness og hændelseshåndtering. IT-sikkerhedsteam håndterer SOC, teknisk drift og it-beredskab.
Rapportering	**Øvrige direktion:** Kvartalsvis rapportering med detaljeret status på NIS2 og informationssikkerhed, herunder compliance, hændelser, audit og leverandørstyring. Rapporten bør være datadrevet og understøtte strategisk beslutningstagning. **Kommunalbestyrelse/fagudvalg:** Halvårlig, eller ved behov, orientering med fokus på strategisk modenhed, governance, hændelser og risikobillede. Kan suppleres med temamøder ved større ændringer eller trusler. **Informationssikkerhedsudvalg:** Mødes månedligt med underudvalg fra hver forvaltning og/eller koordineringsgruppe, som rapporterer kvartalsvist i egne forvaltninger til relevante chef/administrative niveauer. Samlet statusrapport til direktion og audit hvert kvartal eller ved øvrige behov.