2.4 Teknisk målbillede - Compliance

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3

Conscia
Secure progress

De samlede dokumenter er udarbejdet som et arbejds- og referencegrundlag. Videreformidling, kopiering eller anvendelse i andre sammenhænge bør ske med omtanke og med kendskab til dokumentets formål og kontekst. Eventuelle udskrifter betragtes som ukontrollerede.

Indholdsfortegnelse

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

Dette dokument bygger på de arkitekturprincipper, der er fastlagt i hoveddokumentet, og som er kvalificeret gennem en analyse- og workshopfase med deltagelse fra relevante kommunale aktører. Principperne afspejler dermed både et fagligt perspektiv og de erfaringer og behov, der er identificeret på tværs af kommunerne.

Dokumentet består af udvalgte arkitekturprincipper og tilhørende anbefalinger baseret på erfaringer, analyser, best practice og standarder, som vurderes at være centrale for at understøtte en stabil, sikker og robust fælleskommunal IT-drift.

Dokumentet er et fagligt udgangspunkt for det videre arbejde med at etablere en konkret arkitektur og implementeringsplan i den enkelte IT-serviceorganisation. Dette arbejde forudsætter lokal tilpasning og skal gennemføres i samspil med ejerkommunerne samt med inddragelse af eksisterende producenter og leverandører, hvor det er relevant.

Det endelige ambitionsniveau for sikkerhed, drift og servicemodel fastlægges af den enkelte IT-serviceorganisation på baggrund af ejerkommuners behov, prioriteringer og risikovurderinger.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

1 Formål og anvendelsesområde

Dette dokument beskriver en compliance-model for de regionale IT-Serviceorganisationer, der leverer managed services til en gruppe af modtagende organisationer, som alle er klassificeret som væsentlige enheder under NIS2-direktivet (EU 2022/2555). Modellen afklarer ansvarsfordelingen, de tekniske kontrolkrav og de governance-mekanismer, der er nødvendige for at opfylde NIS2 og GDPR med tilhørende anbefalede kontrolrammer og bedste praksis i form af ISO 27001/27002:2022 og CIS Controls v8.1 i en fælles driftsmodel.

Modellen er særligt målrettet scenariet, hvor:

- De regionale IT-serviceorganisationer (herefter: managed service-leverandører, MSP) fungerer som en kritisk forsyningskædepartner i NIS2-forstand.
- De modtagende organisationer – kommunerne – er forpligtede under NIS2 som væsentlige enheder og dermed ansvarlige for at evaluere, stille krav til og kontraktligt regulere MSP'en som led i deres forsyningskædesikkerhed.
- Begge parter er underlagt NIS2's krav om risikobaserede tekniske og organisatoriske foranstaltninger.

Regulatorisk note: NIS2-direktivets **§ 6** kræver udtrykkeligt, at væsentlige enheder adresserer "forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere." MSP'en er dermed ikke blot underlagt egne NIS2-forpligtelser væsentlig enhed som leverandør af administrerede service — kunderne er tillige forpligtede til aktivt at evaluere og kræve det nødvendige sikkerhedsniveau af leverandøren.

2 Regulatorisk grundlag

Compliance-modellen er forankret i tre overlappende referencerammer, der tilsammen danner et sammenhængende kontrollandskab for en NIS2-forpligtet driftsmodel.

2.1 NIS2-direktivet (EU 2022/2555)

NIS2 erstatter det oprindelige NIS-direktiv fra 2016 og indfører skærpede krav til væsentlige og vigtige enheder inden for 18 sektorer. For centraliseringsscenariet er særligt følgende artikler relevante:

- Overordnede risikobaserede cybersikkerhedsforanstaltninger — proportionalitetsprincippet. §6,(1): *(ISO 5.1+5.25)*
- Håndtering af hændelser, herunder forebyggelse, detektion og reaktion. §6,(2)
- Driftskontinuitet, backup og krisestyring. §6,(3): *(ISO 5.29-5.30 + 8.13-8.14)*

- Forsyningskædesikkerhed — direkte relevant for MSP-relationen. §6,(4): *(ISO 5.19-5.23 + 7.11)*
- Sikker anskaffelse, udvikling og vedligeholdelse af net- og informationssystemer. §6,(5): *(ISO 8.8, 8.20-8.22, 8.25-8.34)*
- Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici. §6,(6) *(ISO 5.35-5.36)*
- Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse. §6,(7): *(ISO 5.16-5.18, 6.3, 8.9, 8.19, 8.22)*
- Kryptografi og kryptering. §6,(8): *(ISO 5.24)*
- Personalesikkerhed, adgangskontrol og aktivstyring; MFA-krav. §6,(9): *(ISO 5.9-5.11, 5.15, 6.1-6.8)*
- brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant. §6,(10) *(ISO 5.5, 5.14, 5.17, 5.29-5.30, 7.12, 8.5)*
- Rapporteringsforpligtelser ved hændelser (24-timers indledende underretning til CSIRT; 72-timers endelig rapport). §12/13:
- Ledelsesansvar og uddannelseskrav for ledelsesorgan. §7:

2.2 Risikobaseret tilgang

NIS2 lovgivningen og ISO 27001 lægger op til en risikobaseret tilgang.

Det betyder også, at man ikke kan lave en fast ramme med nogle fastlagte kontroller, der fører til at fastlagt modenhed. Generelt er en modenhedsscore en måling, der tager højde for flere faktorer, hvorfor man ikke kan fastlægge en modenhedsscore på baggrund af de valgte kontroller.

Implementeringen af foranstaltninger (kontroller) skal jvnf. lovgivningen være proportionale i forhold til risikovurderingen. Hvilket betyder, at det bør være risikovurderingen, der sætter rammerne for de risikominimerende foranstaltninger, som organisationen implementerer, og ikke en fiktiv modenhedsscore, som kunne ende med at give en utilstrækkelig risikominimering, hvis den anvendes forkert.

Mapning af kontroller til det tekniske målbillede tjener til at se sammenhængen i arbejdet med det tekniske målbillede og de benyttede kontrolrammer i forhold til ISO, CIS og minimums tekniske standard. Og til at sikre at de tekniske målbilleder rent faktisk adresserer lovgivningen.

Det endelige valg af kontroller, implementeringsgraden og effektiviteten bør basere sig på føromtalte risikovurdering.

2.3 ISO 27001/27002:2022

ISO 27001:2022 etablerer kravene til et Ledelsessystem for informationssikkerhed (ISMS). ISO 27002:2022 udgør det tilhørende kontrolkatalog med 93 kontroller fordelt på fire kategorier. I forsyningskædekonteksten er særligt kapitel 5.19-5.22 relevante (informationssikkerhed i leverandørforhold) samt kapitel 8 (teknologiske kontroller). I forbindelse med konkret efterlevelse af NIS2-lovkrav er det dog ikke alle kontroller, der er i spil. Se ovenfor for ISO-mapping til lovkrav.

2.4 CIS Controls v8.1

CIS Controls v8.1 udgør 18 prioriterede sikkerhedskontroller med tre implementeringsgrupper (IG1 - IG3). For væsentlige enheder med en managed service-leverandør anbefales som minimum Implementeringsgruppe 2 (IG2), som dækker organisationer med IT-kompetencer og et moderat trusselbillede. Samtlige CIS-kontroller er relevante i forhold til NIS2 kravene.

- Fortegnelse over aktiver. #1-2
- Databeskyttelse. #3:
- Konfiguraktionsstyring. #4
- Kontostyring og adgangsstyring. #5-6:
- Kontinuerlig sårbarhedsstyring. #7:
- Auditlog administration.#8:
- Web-browser og malware beskyttelse. #9-10
- Datagendannelse. #11:
- Netværksstyring og sikker netværksovervågning. #12-13:
- Awarenesstræning. #14
- Administration af leverandørrelationer. #15:
- Sikkerhed i applikationsprogrammel. #16
- Håndtering af hændelsesresponset. #17:
- Test og validering af kontroller. #18

2.5 Bedste praksis for anvendelsen af ISO og CIS kontrollerne i sikkerhedsarbejdet

Med ISO får organisationen en standardiseret ramme for håndtering af den samlede informationssikkerhed og risikohåndtering.

Når det gælder de tekniske kontroller, mangler ISO de prioriterede og konkrete kontrolanbefalinger, som sikkerhedseksperter har udviklet over år med fokus på at levere effektiv sikkerhed.

Derfor vælger mange organisationer at anvende ISO27001 og CIS V8.1 i et effektivt samspil, og det er også anbefalingen i forbindelse med de nye driftscentre. Det skal bemærkes, at mange kommuner for længst har adopteret CIS-kontrollerne i arbejdet med at styrke den faktiske sikkerhed i samspil med ISO27001.

2.6 Compliance og sikkerhed

Dette afsnit belyser forskellen mellem compliance og sikkerhed.

Hvis vi ønsker at beskytte vores kritiske aktiver mod et sæt af trusselsaktører, som bliver stadigt mere sofistikerede for at nå deres mål, så gør compliance det ikke alene. Det er vigtigt at forstå dette og forstå, hvad det fordrer for at gøre organisationen **BÅDE COMPLIANT OG SIKKER.**

Compliance er ikke det samme som sikkerhed. To organisationer kan være 100% compliant – men have vidt forskellig reel beskyttelse. Forskellen ligger i, hvordan sikkerhedskontroller implementeres, konfigureres og drives i praksis. Mange virksomheder opfylder kravene på papiret, men mangler den nødvendige dybde, integration og løbende optimering, der reelt stopper moderne trusler. Derfor bør compliance ses som et udgangspunkt – ikke målet – for effektiv cybersikkerhed.

Helt grundlæggende udstikker compliance retning og rammer gennem risikovurdering og politikker, procedurer, processer og retningslinjer.

Uden disse kan man godt bygge sikkerhed, men erfaringen viser at den sikkerhed man bygger har en begrænset levetid, fordi fundamentet (compliancerammen) ikke er på plads til at fastholde den, og derfor skrider sikkerheden langsomt. Sikker i dag – usikker i morgen.

Hvorfor 100% compliance kan give alt fra 25% til 95 % sikkerhedsefficiens i virkeligheden – og hvad du kan gøre ved det?

2.6.1 Compliance og sikkerhed - udfordringen

Hvert år investerer organisationer betydelige ressourcer i at opnå compliance med sikkerhedsrammeværk som CIS-kontroller, ISO 27001 og NIST CSF samt lovkrav som NIS2 og GDPR. Auditrapporter udarbejdes. Bokse krydses af, certifikater udstedes, og alligevel sker der fortsat brud – ofte hos organisationer, der bestod deres seneste audit med bravour.

Den ubehagelige sandhed er denne: Compliance og sikkerhed er ikke det samme. Compliance måler, om en kontrol eksisterer. Sikkerhed afhænger af, hvor effektivt kontrollen faktisk virker. Det er i kløften mellem de to, at organisationer kompromitteres.

2.6.2 Det centrale paradoks

To organisationer kan begge opnå 100% compliance mod den samme CIS-kontrol – og alligevel kan den ene operere med 25% reel sikkerhedseffektivitet, mens den anden ligger på 95%. Forskellen er ikke kun, hvad de har implementeret, men hvordan de har udrullet det. Det er afgørende for den reelle risikominimering, der opnås.

2.6.3 De faktorer, der afgør, hvor effektiv sikkerheden reelt er

Når vi vurderer den reelle efficiens af en implementeret securitykontrol, evaluerer vi den på tværs af syv dimensioner:

- Funktionel dybde – måden løsningen arbejder på; ud over ovenstående har løsningen faktisk bredere dækning inden for rammerne af de foreskrevne safeguards.
- Dækningsgrad ved udrulning – dækker løsningen faktisk alle aktiver i scope eller kun et repræsentativt udsnit?
- Konfigurationsdybde – kører løsningen med standardindstillinger, eller er den hærdet og tunet til miljøet?
- Integration og korrelation – deler løsningen signaler med andre kontroller, eller opererer den isoleret?
- Tuning og baselining – er normal adfærd blevet profileret, så anomalier faktisk detekteres?
- Responsautomatisering – kan kontrollen handle autonomt på trusler, eller genererer den kun alarmer?
- Kontinuerlig forbedring – gennemgås og opdateres kontrollen løbende, eller installeres den og bliver derefter glemt?

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

2.6.4 Områdeeksempler

2.6.4.1 Patch Management (CIS-kontrol 7)

Som minimum scanner en organisation månedligt efter manglende patches og anvender kritiske patches inden for 30 dage. Det opfylder kontrollen. Men hvis patchdækningen kun er 70 % af endpoints, hvis legacy-systemer er udeladt, og hvis der ikke er nogen automatiseret udrulning, opererer organisationen fortsat med betydelig eksponering.

Et korrekt implementeret patch management-program opnår en dækning på over 95 %, automatiserer udrulningen af kritiske patches og integrerer med sårbarhedshåndtering for at prioritere ud fra, hvor let sårbarheder kan udnyttes. Forskellen i den reelle angrebsflade er betydelig.

2.6.4.2 Endpoint Detection & Response (CIS-kontrol 10)

En basal antivirusløsning med signaturopdateringer hver 24. time opfylder teknisk set kravene til malware defence og vil fange gårsdagens kendte trusler. Avancerede antivirusløsninger med avanceret malware-detektering, zero-day-detektering/beskyttelsesevne, beskyttelse mod exploit-teknologier og adfærdsanalyser kan derimod opdage ukendte trusler, fileless attacks, living-off-the-land-teknikker og lateral movement – mønstre, som er usynlige for signaturbaserede værktøjer.

Dækningsgabet mellem disse to implementeringer overstiger let 60 % i detekterings- og beskyttelsesevne over for virkelige trusselsaktørers TTP'er. Samme kryds i compliance-boksen, men et betydeligt gab i efficiens i forhold til det sikkerhedsniveau, der ønskes opnået. Dertil kommer, at en dårligt styret sikkerhedskonfiguration kan gøre begge løsninger ineffektive.

2.6.4.3 Identity & Access Management (CIS-kontrol 5 & 6)

At kontrollere, at MFA er aktiveret, og at der findes en adgangspolitik for privilegerede konti, opfylder compliancekravene. Men hvis MFA kan omgås via legacy-protokoller, hvis servicekonti har for brede rettigheder, og hvis privilegeret adgangskontrol ikke er isoleret gennem en Privileged Access Workstation (PAW)-arkitektur eller en Privileged Access Management (PAM)-løsning, er kontrollen i høj grad blot teater.

Korrekt implementeret IAM med just-in-time access, fuld PAM-integration og løbende adgangskontrol giver en fundamentalt anderledes risikoreduktion.

Måleproblemet

De fleste compliance assessments spørger: "Er denne kontrol på plads?"

Det relevante spørgsmål er: "Hvis en angriber forsøgte at udnytte denne angrebsflade i dag, hvor stor en andel af forsøgene ville denne kontrol faktisk stoppe – og hvor hurtigt?" Dette spørgsmål kræver teknisk vurdering og ikke alene dokumentgennemgang.

Network Security Monitoring (CIS-kontrol 13)

At installere en SIEM og sende firewall logs til den opfylder kravet. Men en SIEM uden tunede detektionsregler, uden adfærdsmæssige baselines og uden korrelation med endpoint- eller Identitetstelemetri skaber en lavine af alarmer, der lammer security teams – og overser de subtile, langsomme trusler, der faktisk betyder noget. En optimeret kapacitet til sikkerhedsmonitoring, der integrerer netværks-, endpoint-, identitets- og cloud-telemetri med kurateret trusselsefterretninger, reducerer mean time to detect (MTTD) med størrelsesordener.

2.6.5 Praktiske anbefalinger

Baseret på vores security assessment-arbejde på tværs af enterprise-miljøer anbefaler vi følgende tilgang for at lukke kløften mellem compliance og efficiens:

- **Etablér efficiensbaselines** – for hver kritisk kontrol skal I definere, hvordan effektivitet ser ud i målbare termer: detekteringsrater, dækningsprocenter, mean time to respond og false-negative-rater. Brug threat modelling og MITRE ATT&CK til at tilpasse jeres sikkerhedsforanstaltninger til de metoder, angribere faktisk bruger, så den reelle sikkerhedsefficiens styrkes.
- **Gennemfør validering med udgangspunkt i realistiske angrebsscenarier** – anvend purple team-øvelser, breach and attack simulation (BAS)-værktøjer eller målrettet penetration testing til empirisk at måle, hvad jeres kontroller faktisk stopper.
- **Auditér konfigurationsdybde, ikke kun tilstedeværelse** – jeres næste compliance review bør inkludere konfigurationsbenchmarking mod CIS Benchmarks eller leverandørens guideline for hærdning – ikke kun spørgsmålet "Er det installeret?"
- **Vurdér leverandør- og løsningsvalg gennem en efficienslinse** – når I evaluerer security-produkter, bør I kræve proof-of-concept-test mod jeres trusselsprofil – ikke marketing-benchmarks fra leverandøren selv.
- **Behandl integration som et kernekrav** – isolerede kontroller er i sagens natur mindre effektive. Kræv derfor indsigt i, hvordan hver løsning integrerer med jeres SIEM, identitetsplatform og incident response-workflow.
- **Genbesøg årligt** – angribernes metoder udvikler sig. En kontrol, der var 90 % effektiv for to år siden, kan være 40 % effektiv mod nutidens angribere, hvis den ikke er blevet opdateret og tunet.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

3 Modelscenariet: Den centraliserede driftsmodel

3.1 Aktørerne i modellen

Compliance-modellen opererer med to primære aktørtyper i en vertikal leverandørrelation:

- **Den centrale driftsorganisation - MSP-leverandøren - der leverer IT-infrastruktur, datacenter-kapacitet, styrede tjenester og sikkerhedsoperationer til kunderne. MSP'en vil typisk selv falde under NIS2's sektor for digital infrastruktur (datacenterudbydere) og er i sig selv underlagt NIS2-forpligtelser.**
- **Organisationer, der aftager MSP-leverandørens ydelser, og som selvstændigt er ansvarlige for overholdelse af NIS2 som væsentlige enheder. De er underlagt et eksplicit krav om at evaluere og stille krav til MSP'en som leverandør i forbindelse med forsyningskædesikkerheden.**

3.2 Det dobbelte compliance-ansvar

Et centralt princip i modellen er, at NIS2-ansvaret ikke kan uddelegeres til MSP'en. Kunden forbliver fuldt ansvarlig overfor tilsynsmyndigheder og kan ikke fraskrive sig dette ansvar ved at pege på MSP'en. Dette medfører et dobbelt compliance-ansvar:

- MSP'en skal implementere og dokumentere sikkerhedskontroller for infrastrukturen og de leverede tjenester — både som led i egne NIS2-forpligtelser og som kontraktuel forpligtelse over for kunderne.
- Kunden skal aktivt evaluere MSP'ens sikkerhedsniveau, stille kontraktuelle krav, indhente beviser (revisionrapporter, certificeringer) og sikre, at MSP'ens kontroller dækker de risici, der er relevante for kundens væsentlige tjenester.

3.3 Tjenestekategorier der dækkes

Modellen er designet til at dække følgende typiske managed service-kategorier i en centraliseret datacenter-opsætning:

- **Compute, storage og netværk.** Infrastructure as a Service (IaaS):
- **Middleware, databaser, containerplatforme.** Platform as a Service (PaaS):
- **SIEM, SOC, sårbarhedsstyring, endpoint-beskyttelse.** Managed Security Services:
- **Replikering, failover og gendannelsestest.** Backup og Disaster Recovery as a Service:
- **IAM, MFA, privilegeret adgangsstyring (PAM).** Identitets- og adgangsstyring:

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

- **Segmentering, firewall-management, Zero Trust Network Access (ZTNA).** Netværksstyring:

4 Forsyningskædesikkerhed under NIS2

4.1 MSP'ens forpligtelser

Som kritisk forsyningskædepartner for ejerkommunerne er MSP'en forpligtet til som minimum at:

- Implementere og vedligeholde et ISMS i overensstemmelse med ISO 27001:2022 og dokumentere dette over for kunderne.
- Tilbyde revisionsmuligheder eller fremvise revisionsrapporter fra uafhængig tredjepart (f.eks. ISO 27001-certifikat, SOC 2 Type II).
- Indgå en databehandleraftale (DPA) i overensstemmelse med GDPR samt et sikkerhedsbilag i overensstemmelse med NIS2 for alle kunder, der behandler personoplysninger som led i de væsentlige tjenester.
- Opretholde en hændelses-responsprocedure, der sikrer varsling af kunder inden for 4 timer ved driftspåvirkende sikkerhedshændelser og understøtter kundens NIS2 §12/13-rapporteringsforpligtelse.
- Levere regelmæssig dokumentation af sikkerhedsopsætning, herunder: penetrationstestrapporter (mindst årligt), sårbarhedsscanningsrapporter (månedligt) og ændringslog.
- Gennemføre business continuity- og disaster recovery-tests mindst kvartalsvist og stille testresultater til rådighed for kunderne.

4.2 Kundens evalueringsforpligtelser

Den modtagende organisation er forpligtet til aktivt at evaluere MSP'en som led i sin forsyningskædesikkerhed:

- Før kontrakt skal kunden gennemføre en struktureret leverandørrisikovurdering, der dækker MSP'ens tekniske, organisatoriske og juridiske sikkerhedsforhold. Indledende vurdering
- Kunden bør løbende overvåge MSP'ens compliance-status, herunder indhente opdaterede certifikater og revisionrapporter mindst årligt. Løbende overvågning
- Kontrakten skal eksplicit regulere: sikkerhedsniveaukrav, hændelsesnotifikationsforpligtelser, revisionsret, ret til at terminere ved væsentlig compliance-brist, samt SLA for tilgængelighed og hændelsesrespons. Kontraktuelle minimumskrav
- Kunden skal kortlægge, hvilke af sine væsentlige tjenester der er afhængige af MSP'ens infrastruktur, og vurdere konsekvensen ved bortfald. Afhængighedsanalyse

- En dokumenteret exit-plan og datamigrationsprocedure skal være på plads, inden MSP-kontrakten underskrives. Exit-strategi*

**Kommentar: Da det ved lov er besluttet, at kunden skal operere i et ved lov besluttet setup, bør det overvejes, om der skal udarbejdes en exitstrategi. Dette bør indgå i ISMS med en begrundet beslutning under henvisning til lovgivningen på området.*

4.3 Kontraktuelle minimumskrav

Kontrakten mellem MSP og kunden skal som minimum indeholde følgende sikkerhedsbestemmelser:

Bestemmelse	Krav
Sikkerhedsniveau	MSP skal til enhvertid opretholde et sikkerhedsniveau der understøtter NIS2 §6 og kontrolforanstaltninger baseret på risikovurdering alternativt anbefales et niveau svarende til CIS IG2 niveau af kontroller
Hændelsesnotifikation	MSP skal notificere kunden med en tidsfrist der sætter kunden i stand til at efterleve lovkravet indenfor de fastsatte tidsrammer.
Revisionsret	Kunden har ret til at iværksætte uafhængig revision af MSP'ens sikkerhedsforanstaltninger med 30 dages varsel
Certifikater og dokumentation	For at kunne dokumentere sikkerhedsniveauet hos MSP kan f.eks. gyldigt ISO 27001-certifikat tjene som dokumentation med en SoA, der afspejler implementeringen af de rette sikkerhedskontroller der flugter med NIS2 kravene, SOC 2 Type II-rapport eller en decideret NIS2 revisor erklæring. Disse bør stilles til rådighed mindst én gang om året
Underleverandørers sikkerhed	MSP's brug af underleverandører kræver kundens forudgående godkendelse; underleverandører er underlagt tilsvarende sikkerhedskrav, så hele kæden er sikret
SLA for tilgængelighed	Minimum 99,9% tilgængelighed; RTO ≤ 4 timer; RPO ≤ 1 time for kritiske systemer, men bør generelt være afhængig af kritikaliteten af de services der leveres.
Dataejerskab og -portabilitet	Kundens data forbliver kundens ejendom; fuld dataportering sikres ved kontraktophør**

Bestemmelse	Krav
Bødeklausul og exit	Manglende opfyldelse af sikkerhedskrav berettiger kunden til at terminere kontrakten med 30 dages varsel uden erstatningspligt**

*** Igen: På grund af den lovmæssige konstruktion kan det diskuteres, om disse generelle krav bør være afspejlet i kontrakten mellem de regionale driftscentre og kommunen.*

5 Governance- og ansvarsmodel

Nedenstående RACI-model (R = Ansvarlig, A = Accountable, C = Konsulteret) angiver fordelingen af ansvar for de centrale complianceaktiviteter. Bemærk, at kundens ansvar ikke kan uddelegeres til MSP'en – kunden forbliver i alle tilfælde Accountable over for tilsynsmyndigheder.

Fra kunde til serviceudbyder:

Aktivitet	Kontrol / Artikel	MSP	Kunde	Begge	Ref.
Risikovurdering og -styring	NIS2 §6(1)		A		§1
Politikker for informationssikkerhed	NIS2 §6(1)		A		§2
Hændelseshåndtering – detektion	NIS2 §6(2)	**R**	C		§3
Hændelsesrapportering (24t/72t)	NIS2 §12/13	C	**R**		§4
Forsyningskædevurdering (leverandør)	NIS2 §6(4)		**R**		§5
Kontraktuelle sikkerhedskrav (SLA/DPA)	NIS2 §6(4)		A		§6
Driftskontinuitet & backup	NIS2 §6(3)	**R**	C		§7
Adgangsstyring & IAM	NIS2 §6(9)	**R**	C		§8
Kryptering & nøglehåndtering	NIS2 §6(8)	**R**	C		§9

Aktivitet	Kontrol / Artikel	MSP	Kunde	Begge	Ref.
Netværkssegmentering & Zero Trust	NIS2 §6(7)	**R**	C		§10
Sårbarhedshåndtering & patch	NIS2 §6(5)	**R**	C		§11
Logning, overvågning & SIEM		**R**	C		§12
Leverandørrevision & auditrapport	NIS2 §6(4)	**R**	A		§13
Compliancedokumentation & beviser	NIS2 §6(1)		**R**	A	§14

Nøgle: R = Responsible (udfører), A = Accountable (ansvarshavende over for myndigheder), C = Consulted (inddrages). Blanke felter indikerer ingen direkte rolle.

5.1 Ledelsesansvar (NIS2 §7)

- Der henvises specifikt til Kommunal NiS2 drejebog om emnet under ledelsesansvar.

6 Teknisk kontrol-mapping

Nedenstående tabel præsenterer en konsolideret mapping af de centrale sikkerhedsdomæner med tilhørende referencer til NIS2, ISO 27002:2022 og CIS Controls v8.1. Tabellen kan anvendes direkte som dokumentationsgrundlag i forbindelse med ISO 27001-certificering og NIS2-rapportering.

Sikkerhedsdomæne	NIS2 Art. 21	ISO 27001/2:2022	CIS Controls v8.1	Beskrivelse
Risikovurdering	§6	5.1, 6.2		Løbende risikovurdering af centraliserede og kunderelaterede aktiver
Forsyningskædesikkerhed	§6(4)	5.19-5.22	#15	Kontraktuel regulering; leverandørvurdering; revisionsret
Hændelseshåndtering	§6(2) + §12/13	5.24-5.28	#8, #13, #17	Detektion, triagering, rapportering (24t til CSIRT, 72t endeligt)
Adgangsstyring & IAM og håndtering af aktiver	§6(9)	5.15-5.18, 8.2-8.5	#5, #6, #1, #2	MFA, least privilege, privilegeret adgangsstyring (PAM)
Kryptografi & databeskyttelse	§6(8)	8.24-8.26	#3	Kryptering i transit og hvile; nøglehåndteringsprocedure
Netværkssikkerhed & segmentering	§6(7)	8.20-8.23	#12, #13	Zero Trust-arkitektur; mikrosegmentering; DMZ; multi-tenant isolation
Driftskontinuitet & backup	§6(3)	5.29-5.30, 8.13	#11	RTO/RPO-garantier; krypterede offline-backup; DR-tests kvartalsvis
Sårbarhedsstyring	§6(5)	8.8, 8.19	#7	Patch SLA: kritisk <72t; høj <7d; scanning månedligt

Sikkerhedsdomæne	NIS2 Art. 21	ISO 27001/2:2022	CIS Controls v8.1	Beskrivelse
Logning & overvågning	§6(2)+(5)	8.15-8.16	#8	SIEM-centralisering; logopbevaring min. 12 mdr.; korrelationsregler
Sikker konfiguration	§6(7)	8.9, 8.19	#4	Baseline-konfigurationer; hardening-standarder (CIS Benchmarks)
Personalesikkerhed	§6(9)	6.1-6.6	#14	Sikkerhedsgodkendelse; NDA; awareness-uddannelse mindst årligt
Cyberhygiejne & uddannelse	§6(7)	6.3	#14	Phishing-tests; obligatorisk NIS2-træning til ledelse

6.1 Kritiske tekniske kontroller for MSP'en

Ud over den generelle mapping anbefales følgende specifikke tekniske foranstaltninger for en MSP, der betjener væsentlige enheder:

6.1.1 Multi-tenant isolation og netværkssegmentering/segregering

I et scenarie med adskillige væsentlige kunder på fælles infrastruktur er det afgørende, at MSP'en implementerer:

- Logisk isolation af kundemiljøer ved brug af VLAN, VRF, VxLAN eller tilsvarende teknologier.
- Effektiv adskillelse med FW mellem VLAN/VRF/VxLAN - filtrering
- Zero Trust Network Access (ZTNA) som arkitekturelt princip: ingen implicit tillid internt i netværket. Least privilege adgangskontrol i netværket med brug af identiteter.
- Strenge east-west traffic-kontroller for at forhindre lateral bevægelse på tværs af kundemiljøer og mellem applikationer i kundens specifikke tenant.
- Separate management-planer for hver kunde.

6.1.2 Sikkerhedsovervågning og SIEM

MSP'en bør tilbyde — og kunden bør kræve — centraliseret sikkerhedsovervågning med:

- Logindsamling fra alle kunders systemer med minimum 12 måneders retention.
- Korrelationsregler for kritiske angrebsvektorer (brute force, lateral movement, exfiltration).
- Definerede SLA'er for alarmtid: kritisk alarm ≤ 15 minutter, høj alarm ≤ 1 time.
- Månedlig trussels- og hændelsesrapportering til kunden.

6.1.3 Privilegeret adgangsstyring (PAM)

- Alle privilegerede konti (admin, systemadmin) skal håndteres i en PAM-løsning med just-in-time-adgang.
- MFA er påkrævet for alle adgangstyper, der vedrører produktionsmiljøer.
- Session recording for privilegerede sessioner.
- Automatisk deaktivering af inaktive konti efter 30 dage.

7 Revision og løbende håndhævelse

7.1 Intern revision

MSP'en bør gennemføre interne revisioner af ISMS mindst én gang om året med fokus på de kontroller, der er mest relevante for kundernes væsentlige tjenester. Revisionsrapporterne stilles til rådighed for kunderne på anmodning.

7.2 Tredjeparts-revision og certificering

Det anbefales, at MSP'en opretholder:

- ISO 27001-certificering, der inkluderer de leverede managed services i scope.
- SOC 2 Type II rapport, der dækker Trust Service Criteria for Security, Availability og Confidentiality (sikkerhed, tilgængelighed og fortrolighed).
- Penetrationstest af kritisk infrastruktur mindst én gang om året foretaget af akkrediteret tredjepart.

7.3 Tilsynsmyndighedens krav til kunden

Kunden skal ved tilsynssager kunne dokumentere:

- At der er gennemført en leverandørrisikovurdering af MSP'en inden kontrakt.
- At kontrakten indeholder NIS2 kompatible sikkerhedskrav.
- At MSP'ens compliance status vurderes løbende og minimum én gang om året.

- At hændelsesrespons- og notifikationsprocedurer er testet.
- At der foreligger en opdateret afhængighedskortlægning.

8 Konklusion og implementeringsrækkefølge

Implementeringen af compliance modellen anbefales gennemført i følgende faser:

Fase	Aktivitet	Indhold	Tidshorisont
1	**Fundament**	Etabler ISMS (ISO 27001), godkend sikkerhedspolitik, gennemfør indledende risikovurdering. Kortlæg væsentlige tjenester og afhængigheder til MSP.	0-3 måneder
2	**Leverandørscreening**	Gennemfør struktureret MSP vurdering vha. scoringsmodellen (kap. 7). Identificer huller og forhandl kontraktuelle sikkerhedskrav (kap. 4.3).	1-4 måneder
3	**Teknisk implementering**	Implementer tekniske kontroller: MFA, PAM, netværkssegmentering, SIEM, backup/DR. Verificer multi-tenant isolation med MSP.	3-9 måneder
4	**Test og dokumentation**	Gennemfør DR tests, penetrationstest og hændelsesresponsøvelser. Byg compliancedokumentation til tilsynsmyndigheder.	6-12 måneder
5	**Kontinuerlig forbedring**	Løbende overvågning, kvartalsvis gennemgang, årlig revision og opdatering af risikovurdering. Genscor MSP'en halvårligt.	Løbende

Denne compliance model udgør et levende dokument, der bør opdateres i takt med ændringer i det regulatoriske landskab, trusselsbilledet og MSP konstellationen. ENISA udgiver løbende teknisk vejledning, og den danske implementering af NIS2 kan medføre sektorspecifikke præciseringer.

9 Appendiks A: Referenceliste

- EU 2022/2555 — NIS2 direktivet (CELEX 32022L2555)
- Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau — dansk implementering (CL)
- ISO/IEC 27001:2022 — Krav til informationssikkerhedsstyringssystemer
- ISO/IEC 27002:2022 — Kontroller for informationssikkerhed
- CIS Controls v8.1 — Center for Internet Security (2024)

- ENISA: Technical Implementation Guidance on Cybersecurity Risk Management Measures (2024)
- Digitaliseringsstyrelsen: Tekniske minimumskrav (2025)
- Vejledning til implementering af cybersikkerhedsforanstaltninger — CFCS/Center for Cybersikkerhed

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.