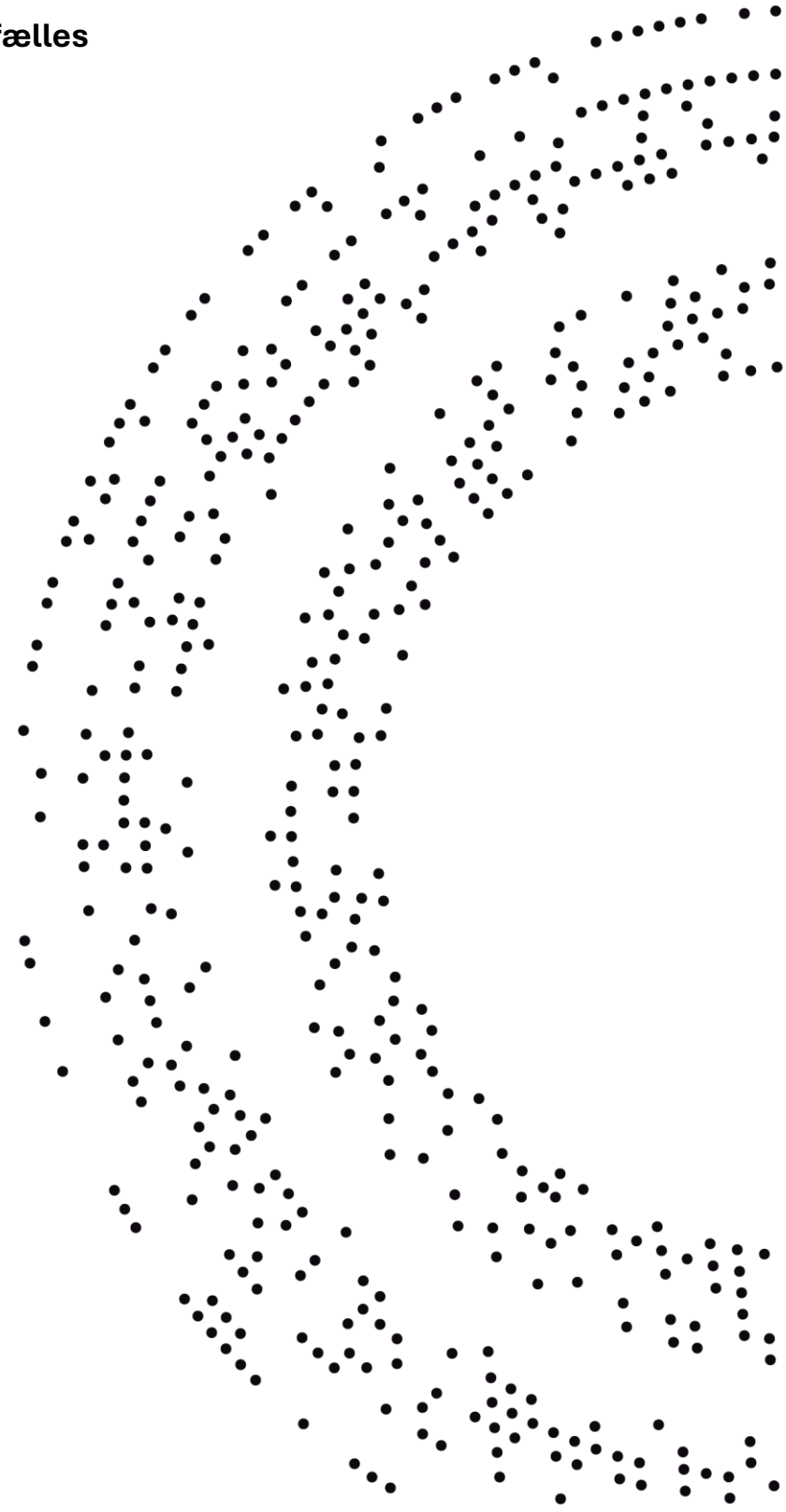
2.4.1 Compliance Kortlægning

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3



Conscia
Secure progress

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.

Indholdsfortegnelse

1 Indledning

Dette dokument udgør en samlet compliance kortlægning for det fælleskommunale tekniske målbillede og fungerer som et arbejds- og referencegrundlag for kommuner og IT-serviceorganisationer i forbindelse med konsolidering og fælles drift.

Dokumentet tager udgangspunkt i Teknisk Målbillede – Hoveddokumentet samt de 15 fælles arkitekturprincipper, der på tværs af sikkerhed, standardisering, konsolidering og segmentering definerer den ønskede målarkitektur. Formålet er at synliggøre, hvordan disse arkitekturprincipper konkret understøtter og opfylder centrale compliance-krav, herunder:

- NIS2-loven (dansk implementering)
- ISO/IEC 27001:2022 og ISO/IEC 27002:2022
- CIS Controls v8.1
- Tekniske minimumskrav

Compliance kortlægningen er ikke tænkt som en erstatning for kommunernes egne risikovurderinger, ISMS-dokumentation eller ledelsesrapportering. Den fungerer derimod som et teknisk translations- og sammenkoblingslag, der forbinder overordnede lov- og standardkrav med de konkrete arkitektur- og designvalg, der er beskrevet i målbillede dokumenterne:

- Teknisk Målbillede – Hoveddokument
  Fastlægger vision, scope og de 15 arkitekturprincipper som en fælles styringsramme.

- 2.1 Teknisk Målbillede – Sikkerhed
  Uddybning af arkitekturprincipper inden for sikkerhed, herunder Security by Design, systemkategorisering, overvågning og Zero Trust.

- 2.2 Teknisk Målbillede – LAN/WAN
  Konkretisering af netværksarkitektur, segmentering, topologier og standardisering.

- 2.3 Teknisk Målbillede – Driftsplatform
  Beskrivelse af driftsplatformens opbygning, modenhed, resiliens, automatisering og multi-tenant drift.

I denne compliance kortlægning er arkitekturprincipperne anvendt som fælles referenceakse, hvor hvert princip mappes systematisk mod relevante krav fra lovgivning og standarder. Dermed skabes en rød tråd fra strategisk arkitektur, over teknisk design og drift, til dokumenterbar compliance.

Læsevejledning

Dokumentet er struktureret i fire hovedgrupper svarende til de fælles arkitekturprincipper:

- Gruppe A – Sikkerhed
- Gruppe B – Standardisering
- Gruppe C – Konsolidering
- Gruppe D – Segmentering

For hvert arkitekturprincip præsenteres:

- konkrete fokusområder
- et vurderet modenhedsniveau
- entydige referencer til NIS2 bestemmelser, ISO kontroller, CIS Controls og tekniske minimumskrav

Modenhedsniveauerne anvendes som et fælles sprog for dialog og prioritering og er direkte koblet til de modenhedsmodeller, der anvendes i de øvrige målbillede dokumenter.

Til sidst findes referencetabeller for :

- NIS2 loven (dansk lov §§)
- ISO 27001/27002:2022
- CIS Controls v8.1
- Tekniske minimumskrav

2 Compliance kortlægning pr. arkitekturprincip

Gruppe A — Sikkerhed

A1 — Security by Design og Sikkerhedsmodenhed

Sikkerhed integreres som en grundlæggende del af arkitekturen. Ansvarsmodeller, hardening, serviceeksponering, DNS sikkerhed og firewall governance er definerede, dokumenterede og håndhævede. Kilde: 2.1.1 Teknisk målbillede — Sikkerhed.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
SbD-1	Ansvarsmodel for drift og sikkerhed — RACI, shared responsibility, kommunegrænser	§7, §6,stk.1	5.2, 5.36, 5.37	N/A	—
SbD-2	Hardening af infrastrukturkomponenter — CIS Benchmarks, godkendt baseline, afvigelseshåndtering	§6,stk.5	8.9, 8.19	CIS 4.1, CIS 4.2, CIS 4.6	Krav 5, Krav 7, Krav 29
SbD-3	Risikobaseret tilgang til serviceeksponering — screening, Zero Trust-principper, eksponeringsregister	§6,stk.1, §6,stk.5	5.9, 8.20, 8.27	CIS 7.2, CIS 12.2	Krav 26, Krav 27, Krav 28
SbD-4	Ensartet sikkerhedsniveau på tværs af kommuner — centralt internet exit, DDoS beskyttelse, SASE	§6,stk.1	5.1, 5.36	CIS 4.1, CIS 12.2	—
SbD-5	DNS sikkerhed — DNSSEC-signing, C2-filtrering, intern/ekstern DNS adskillelse	§6,stk.1, §6,stk.5	8.20, 8.21	CIS 4.9, CIS 9.2, CIS 13.4	Krav 17, Krav 18, Krav 21, Krav 22
SbD-6	Firewall management og regelbase — deny-by-default, formel styringsproces, change management	§6,stk.1, §6,stk.5	8.20, 8.21, 8.22	CIS 4.4/4.5, CIS 12.2, CIS 12.4, CIS 13.4	Krav 1, Krav 25
SbD-11	Compliance med s tekniske minimumskrav — komplet kortlægning, dashboard, kvartalsvis status	§6,stk.1, §6,stk.6	5.1, 5.36	CIS v8.1	Krav 1–29 (alle)
SbD-12	Netværksdokumentation og konfigurationsstyring — komplet, versionsstyret, opdateret topologi	§6,stk.1, §6,stk.5	5.37, 8.9, 8.20	CIS 4.2, CIS 12.4	—

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
SbD-13	Regelbase governance og firewall audit — kvartalsvise audits, forældelsesoprydning, versionsstyring	§6,stk.1, §6,stk.6	8.20, 5.35	CIS 4.4/4.5, CIS 13.4.	Krav 1, Krav 25

A2 — Kategorisering af IT-systemer

Alle systemer registreres i CMDB, klassificeres, livscyklusstyres og segmenteres på baggrund af klassifikationen. Dokumentation holdes komplet og opdateret. Kilde: 2.1.1 Teknisk målbillede — Sikkerhed og 2.2.1 LAN/WAN.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Kat-1	Registreringsdækning og -kvalitet — komplet inventar: hardware, software, cloud, OT	§6,stk.1	5.9, 5.10	CIS 1.1, CIS 1.2, CIS 2.1	—
Kat-2	Livscyklusstyring og -mærkning — EOL-styring, planlagt udfasning, automatisk CMDB opdatering	§6,stk.1, §6,stk.5	5.12, 8.8	CIS 1.1, CIS 1.3, CIS 2.1, CIS 2.4	Krav 5, Krav 7, Krav 29
Kat-3	Netværksdokumentation — logisk og fysisk topologi, versionsstyret, kvartalsopdateret	§6,stk.1	5.37, 8.20	CIS 12.4	—
Kat-4	Sikkerhedsdokumentation — risikovurderinger, sikkerhedspolitikker, review cyklus	§6,stk.1, §6,stk.6	5.1, 5.35, 5.36	CIS v8.1	—
Kat-5	Driftdokumentation — runbooks, SOP, beredskabsplaner, offline tilgængelighed	§6,stk.1	5.37	CIS 17	—
Kat-6	Ensartet klassifikationsbrug — fælles taksonomi på tværs af kommuner, ISO 27001-alignet	§6,stk.1	5.12, 5.13	CIS 1.1, CIS 2.1, CIS 3.7	—
Kat-7	Struktureret CMDB platform — CI-relationer, automatisk discovery, ITSM integration	§6,stk.1	5.9, 5.10	CIS 1.1, CIS 2.1, CIS 3.2	—
Kat-8	Netværkssegmentering baseret på systemklassifikation — VLAN, zoner, VRF pr. klasse	§6,stk.5	8.20, 8.22	CIS 12.2	Krav 25
Kat-9	Redundans og kritikalitetsmærkning — kritikalitetsklassificering, redundanskrav pr. klasse	§6,stk.3	8.14, 5.29, 5.30	CIS 11.2	—
Kat-10	Afhængighedskortlægning — applikations-/serviceafhængigheder, forsyningskæde	§6,stk.1, §6,stk.4	5.9, 5.21	CIS 1.1, 2.1, CIS 3.8, CIS 15.1	—

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Kat-11	API-adgang til systemregister — machine readable inventory, CMDB integration, rapportering	§6,stk.1, §6,stk.5	5.37, 8.9	CIS 1.1, CIS 2.1	—
Kat-10b	Kategorisering af systemer (LAN/WAN-kontekst) — netværksniveau klassifikation, sikkerhedszonetildeling	§6,stk.1	5.9, 5.12	CIS 1.1, CIS 12.2, CIS 12.4	—

A3 — Overvågning og auditering

Komplet logindsamling fra alle relevante logkilder. Centraliseret SIEM, NOC-funktion, telemetri og overvågning af netværk og infrastruktur. Kilde: 2.1.1 Teknisk målbillede — Sikkerhed og 2.2.1 LAN/WAN.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Ovr-1	Logkilderegister — komplet dækning: netværk, servere, cloud, endpoints, applikationer	§6,stk.1, §6,stk.2	8.15, 8.16	CIS 8.1	Krav 16
Ovr-2	Netværkstelemetri — NetFlow/IPFIX fra alle kritiske enheder og perimeter	§6,stk.2	8.16, 8.20	CIS 13.6	Krav 16
Ovr-3	Telemetri pipeline — centraliseret log-routing, normalisering, parsning og filtrering	§6,stk.2, §6,stk.5	8.15, 8.16	CIS 8.1, CIS 8.9	Krav 16
Ovr-4	Log- og transportformat standardisering — CEF/JSON/syslog RFC5424 over TLS	§6,stk.1, §6,stk.2	8.15, 8.17	CIS 8.1	Krav 16
Ovr-5	Tidsynkronisering — NTP/NTS, UTC-stempling på alle logkilder, drift < 1 sekund	§6,stk.1	8.17	CIS 8.4	Krav 16
Ovr-6	Log opbevaring — warm/cold-arkiv, min. 12 måneder retention, immutability og kryptering	§6,stk.1, §6,stk.2	8.15, 5.33	CIS 8.10	Krav 16
Ovr-7	Alarmering og NOC-funktion — centraliseret, prioritetsklassificeret, eskalationsveje	§6,stk.2	8.16	CIS 13.1, CIS 13.3, CIS 13.6	—
Ovr-8	SIEM-implementering — aktiv regelbase, korrelation, triage, playbooks, threat intelligence	§6,stk.2	8.15, 8.16	CIS 13.1	Krav 16
Ovr-9	Overvågning, auditering og SIEM (netværksinfrastruktur) — syslog/SNMP til SIEM, alarmering	§6,stk.2	8.15, 8.16	CIS 8.1, CIS 13.1, CIS 13.3	Krav 16
Ovr-10	Netværksovervågning (NMS) — performance baselines, kapacitetstrends, proaktiv fejldetektion	§6,stk.2	8.16, 8.20	CIS 8.11, CIS 13.1, CIS 13.3	—

Gruppe B — Standardisering

B4 — Adressetildeling og DNS arkitektur

Hierarkisk IP-adresseplan med IPAM-governance. Centraliseret DHCP, DNS arkitektur med DNSSEC og routing designet med redundans. Kilde: 2.2.1 Teknisk målbillede — LAN/WAN, Kategori 3: Adressering og routing.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Adr-1	IP-adresseplan, IPAM og governance — centraliseret, hierarkisk plan (IPv4/IPv6), konfliktstyring	§6,stk.1	5.37, 8.20	CIS 12.2	—
Adr-2	Håndtering af adresseoverlap — proaktiv detektion, VRF instans niveau håndtering ved konsolidering	§6,stk.5	8.20	CIS 12.3	—
Adr-3	DHCP-design og IP-sporbarhed — centraliseret DHCP, logning af adresse-/MAC-binding, forensisk sporbarhed	§6,stk.1, §6,stk.2	8.15, 8.20	CIS 1.4, CIS 8.1, CIS 8.2, CIS 12.3, CIS 13.6	Krav 16
Adr-4	DNS arkitektur og delegation — intern/ekstern adskillelse, DNSSEC, redundante resolvere, formel delegation	§6,stk.5	8.20, 8.21	CIS 4.9, CIS 9.2, CIS 12.2	Krav 17, Krav 18, Krav 21, Krav 22
Adr-5	Routingdesign og redundans — OSPF/BGP, automatisk failover, loop-fri topologi, BFD-timers	§6,stk.3	8.14, 8.20	CIS 12.2	—

B5 — Zonemodeller og Zero Trust

Standardiseret zonemodel med klassifikationsbaseret placering, DMZ-arkitektur og Zero Trust-principper: identitetssikring, MFA, device trust, PAM og deny-by-default. Kilde: 2.1.1 Zoneinddeling & Zero Trust og 2.2.1 Segmentering.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Zon-1	Zone/segmenteringsmodel — formaliseret model, dokumenteret, konsistent implementering	§6,stk.5	8.20, 8.22	CIS 12.2, CIS 12.6	Krav 25
Zon-2	Klassifikationsbaseret zoneplacering — systemkategori afgør placering og restriktioner automatisk	§6,stk.1, §6,stk.5	5.12, 8.22	CIS 12.2	—
Zon-3	DMZ-arkitektur og ekstern eksponeringsstyring — reduceret attack surface, dobbelt firewall, WAF	§6,stk.5	8.20, 8.22	CIS 12.2, CIS 13.4	Krav 26, Krav 27, Krav 28
Zon-4	Identitetssikring af brugere og adgang — IdP integration, brugerlivscyklus, decertificering	§6,stk.9, §6,stk.10	5.15, 5.16, 5.17	CIS 5	Krav 6, Krav 11
Zon-5	MFA og konditional access — obligatorisk MFA, risikobaseret adgang, FIDO2/moderne metoder	§6,stk.10	5.17, 8.5	CIS 6.3, CIS 6.4, CIS 6.5	Krav 11
Zon-6	Sikring af trafik — TLS 1.3 end-to-end, IPsec, krypteret east-west trafik	§6,stk.8, §6,stk.5	8.20, 8.24	CIS 3.10, CIS 12.2	Krav 9, Krav 27
Zon-7	Device trust og endpoint compliance — NAC, zero-trust device posture, compliance-verifikation	§6,stk.5, §6,stk.10	8.1, 8.5	CIS 1.1, CIS 4.1, CIS 13.9	Krav 1, Krav 2
Zon-8	Gæsteadgangsstyring — isoleret gæstenet, tidsbegrænset adgang, ingen intern routing	§6,stk.5, §6,stk.9	5.15, 8.20	CIS 12.2, CIS 13.4	Krav 24, Krav 25
Zon-9	PAM og administrativ adgang — JIT, session recording, just-enough access, centraliseret PAM	§6,stk.9, §6,stk.10	5.15, 5.18, 8.2	CIS 5.4, CIS 6.8	Krav 6, Krav 11
Zon-10	AD-federering og fælles PKI — federeret AD, certifikatlivscyklus, CRL/OCSP, automatisk fornyelse	§6,stk.10	5.16, 5.17	CIS 4.1	Krav 11
Zon-11	Workloads i datacenteret — mikrosegmenteret zoneplacering, identity baserede politikker	§6,stk.3, §6,stk.5	8.27, 8.14	CIS 3.12, CIS 12.2	—

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Zon-12	Deny by default — al trafik afvises som udgangspunkt, eksplicit tilladelsesmodel på alle zonegrænser	§6,stk.5	8.20, 8.21	CIS 4.4/4.5, CIS 12.2, CIS 13.4	Krav 1, Krav 25
Zon-13	Security by Design og zonemodeller (LAN/WAN) — integreret sikkerhed fra designfasen	§6,stk.5	8.20, 8.22, 8.27	CIS 12.2	Krav 25
Zon-14	NAC og endpoint-compliance (LAN/WAN) — 802.1X, enhedscertificering, karantænezon	§6,stk.5, §6,stk.10	8.1, 8.20	CIS 1.1, CIS 4.1, CIS 12.2, CIS 12.6, CIS 13.9	Krav 2

B6 — Logiske netværksstrukturer

Modulært og hierarkisk netværksdesign, hardware lifecycle, WAN-teknologi med kryptering og sikker management-adgang til netværksinfrastruktur. Kilde: 2.2.1 LAN/WAN, Kategori 1 (Netværksarkitektur), 4 (WAN) og 5 (Management).

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Net-1	Modulært og skalerbart netværksdesign — blokbaseret arkitektur, klart definerede moduler	§6,stk.5	8.20, 8.27	CIS 12.2	—
Net-2	Hierarkisk netværksmodel — konsistent tre-lags struktur (core/distribution/access)	§6,stk.5	8.20, 8.22	CIS 12.2	—
Net-3	Ensartede og skalerbare topologier — standardiserede designs på tværs af kommuner og fællesskaber	§6,stk.1, §6,stk.5	5.37, 8.20	CIS 12.2	—
Net-4	Hardware-standardisering og lifecycle — EOL-styring, replacement-plan, dual-vendor strategi	§6,stk.5	8.8, 5.9	CIS 1.1	Krav 5, Krav 26, Krav 29
Net-5	Navngivning, labeling og tagging — konsistente konventioner, automatiseret CMDB integration	§6,stk.1	5.9, 5.13	CIS 1.1, CIS 2.1, CIS 3.2	—
Net-6	WAN-teknologi og kryptering — MPLS/SD-WAN, IPsec/MACsec, krypteret transport end-to-end	§6,stk.8	8.20, 8.24	CIS 12.2, CIS 3.10	Krav 9, Krav 27
Net-7	QoS og trafikprioritering — end-to-end QoS, prioritering af kritiske services og nødkommunikation	§6,stk.3	8.20	CIS 12.2	—
Net-8	Sikker management — out-of-band management net, krypteret CLI/API-adgang, dedikeret netværk	§6,stk.9, §6,stk.10	8.2, 8.20	CIS 12.3	Krav 2, Krav 11
Net-9	AAA og adgangsstyring til netværksudstyr — TACACS+/RADIUS, RBAC, MFA, centraliseret forvaltning	§6,stk.9, §6,stk.10	5.15, 5.18, 8.5	CIS 12.5, CIS 6.5	Krav 6, Krav 11

B7 — Redundansprincipper (Netværk og WAN)

Systematisk redundans i WAN-opkoblinger, kritiske fysiske komponenter og services. Backup af infrastrukturkonfigurationer og WAN-failover med dokumenterede RTO/RPO-mål. Kilde: 2.1.1 Resiliens og 2.2.1 WAN og transport.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Red-1	Redundans i kommunernes WAN-opkoblinger — dual carrier, fysisk uafhængige ruter, testet failover	§6,stk.3	8.14, 5.29, 5.30	CIS 12.2	—
Red-2	Redundans i kritiske fysiske komponenter — HA-konfiguration, dual power, UPS, N+1 kapacitet	§6,stk.3	8.14, 5.29	CIS 12.2	—
Red-3	Redundans i kritiske services — load balancere, softwareredundans (AD, DNS), failover-test	§6,stk.3	8.14, 5.30	CIS 12.2	—
Red-4	Backup og recovery af infrastrukturkonfigurationer — daglig backup, immutable, offline runbooks	§6,stk.3	8.13, 5.29, 5.30	CIS 11.1, CIS 11.2, CIS 11.3, CIS 11.4	—
Red-5	WAN-redundans og resiliens (LAN/WAN) — redundante og diversificerede WAN-forbindelser	§6,stk.3	8.14, 5.30	CIS 12.2	—
Red-6	Optimal ressourceudnyttelse WAN — båndbreddeovervågning, kapacitetsstyring, QoS-måling	§6,stk.3	8.6, 8.20	N/A	—

Gruppe C — Konsolidering

C8 — Datacentre med Multi-tenancy

Logisk tenant-adskillelse via VRF og ressourcepools. Standardiseret onboarding/offboarding, SLA-styring, chargeback og adgangsstyring på tværs af tenanter. Kilde: 2.3.1 Driftsplatform og 2.2.1 LAN/WAN.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Ten-1	Multi-tenancy og makrosegmentering — VRF baseret end-to-end kommuneadskillelse, GDPR-isolering	§6,stk.5	8.20, 8.22	CIS 3.12, CIS 12.2, CIS 13.4,	Krav 25
Ten-2	Logisk tenant-adskillelse — automatiseret håndhævelse af ressourcepools med grænser	§6,stk.4, §6,stk.5	8.22, 5.19	CIS 12.2	—
Ten-3	Tenant-onboarding & offboarding — standardiseret, automatiseret, verificeret og dokumenteret	§6,stk.9	5.16, 5.18	CIS 12.3	—
Ten-4	Chargeback og ressourcerapportering — faktisk forbrug pr. tenant, månedlig transparensrapport	§6,stk.6	5.36	CIS 15.6	—
Ten-5	SLA-styring og governance — KPI'er, månedlig rapport, proaktiv risikostyring, eskalationsmodel	§6,stk.4, §6,stk.6	5.20, 5.22	CIS 15.2	—
Ten-6	Adgangsstyring multi-tenant — RBAC, MFA, JIT, kvartalsvise adgangsreview, zero-standing access	§6,stk.9, §6,stk.10	5.15, 5.18, 8.2	CIS 5.1, CIS 5.2, CIS 5.4, CIS 6.1, CIS 6.5, CIS 6.7, CIS	Krav 6, Krav 11

C9 — Redundans og Resiliens (Driftsplatform)

Multi-site datacenterdesign, compute- og storage-redundans, immutable backup og dokumenterede DR-planer med regelmæssig test. Kilde: 2.3.1 Modenhedsvurdering — Driftsplatform, Redundans & Resiliency.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Res-1	Multi-site datacenter-design — aktiv/aktiv, witness-site, N-1 kapacitet, geografisk adskillelse	§6,stk.3	5.29, 5.30, 8.14	N/A	—
Res-2	Compute-redundans og failover — HA-klynger, admission control, automatisk failover, test	§6,stk.3	5.29, 8.14	N/A	—
Res-3	Storage-replikering og data-resiliency — differentierede RPO/RTO pr. system, halvårlig test	§6,stk.3	5.29, 8.13, 8.14	CIS 11.1, CIS 11.2, CIS 11.3	—
Res-4	Backup og immutability — write-once-backup, offsite replikering, krypteret arkivering, ransomware beskyttelse	§6,stk.3	8.13, 5.33	CIS 11.1, CIS 11.2, CIS 11.3, CIS 11.4	—
Res-5	DR-planer og test — dokumenterede beredskabsplaner, årlig fuld DR-test, målt RTO/RPO	§6,stk.3	5.29, 5.30	CIS 11.3, CIS 11.5	—

C10 — Ensartede og skalerbare topologier

Standardiserede konfigurationer, navngivningskonventioner, versionsstyret dokumentation og designstandarder på tværs af driftsplatform og netværksinfrastruktur. Kilde: 2.3.1 Standardisering og 2.2.1 Governance.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Top-1	Navngivning & labelling (platform) — CMDB drevet, automatisk håndhævelse, ensartet på tværs	§6,stk.1	5.9, 5.13, 5.37	CIS 1.1, CIS 2.1	—
Top-2	Konfigurationsstandarder og baseline-compliance — dokumenteret, auditeret, automatiseret håndhævelse	§6,stk.1, §6,stk.5	8.9, 5.37	CIS 4.1, CIS 4.2, CIS 4.6	Krav 5, Krav 7, Krav 29
Top-3	Hardware-standardisering og lifecycle (netværk) — fælles vendor-strategi, EOL-plan, replacement cyklus	§6,stk.5	8.8, 5.9	CIS 1.1	Krav 5, Krav 26, Krav 29
Top-4	Konfigurationsstyring og versionering (netværk) — GitOps, drift-detection, automatisk remediation	§6,stk.1, §6,stk.5	8.9, 5.37	CIS 4.1, CIS 4.2	—
Top-5	Dokumentation og designstandarder — arkitekturdokumentation, designvejledninger, review cyklus	§6,stk.1	5.37	CIS 4.1, CIS 12.4	—
Top-6	Konsolideringsparathed og transition — migrationsplan, kortlægning af overlappende net, risikovurdering	§6,stk.1, §6,stk.6	5.35, 5.36	N/A	—

C11 — Optimal udnyttelse af ressourcer

Compute rightsizing, storage-optimering, hærdede VM-skabeloner og kapacitetsplanlægning med forecasting. Kilde: 2.3.1 Optimal ressourceudnyttelse og 2.2.1 WAN.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Opt-1	Compute-konsolidering og rightsizing — monitoreringsbaseret, zombie-cleanup, dynamisk justering	§6,stk.3	8.6	N/A	—
Opt-2	Storage-optimering og deduplikering — thin provisioning, deduplikering, tiering, lifecycle-styring	§6,stk.3	8.6, 8.13	N/A	—
Opt-3	Servicekatalog og hærdede VM-skabeloner — CIS-hærdet, versionsstyret, standardiserede images	§6,stk.1, §6,stk.5	5.37, 8.9	CIS 4.1, CIS 4.2	Krav 5, Krav 7, Krav 29
Opt-4	Kapacitetsplanlægning og forecasting — 12-måneders fremskrivning, trendanalyse, proaktiv dimensionering	§6,stk.3	8.6, 5.30	N/A	—
Opt-5	Optimal ressourceudnyttelse WAN — båndbreddemonitorering, QoS, kapacitetsstyring	§6,stk.3	8.6, 8.20	N/A	—

C12 — Automatisering og Infrastructure as Code

IaC og versionsstyret netværkskonfiguration, CMDB integration, self-service og automatiseret drift. Kilde: 2.3.1 Standardisering og 2.2.1 Governance og automatisering.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Aut-1	Infrastructure-as-Code (IaC) og versionsstyring — CI/CD pipelines, GitOps, deklarative konfigurationer	§6,stk.5	8.9, 5.37	CIS 4.6, CIS 12.3	—
Aut-2	CMDB og asset management — CI-relationer, kvartalsvurdering, automatisk discovery, API integration	§6,stk.1	5.9, 5.10	CIS 1.1, CIS 1.2, CIS 2.1	—
Aut-3	Automatiseret drift og self-service portal — event-drevet, runbooks, katalogstyret, brugervenlig	§6,stk.5	5.37, 8.9	N/A	—
Aut-4	IaC og netværks-automatisering — Ansible/NETCONF/RESTCONF, network-as-code, repetérbare deployments	§6,stk.5	5.37, 8.9	CIS 4.6, CIS 12.3	—
Aut-5	Konfigurationsstyring og versionering (netværk) — automatisk backup, drift-detection, compliance-alarm	§6,stk.1, §6,stk.5	8.9, 5.37	CIS 4.6, CIS 12.3	—
Aut-6	Konsolideringsparathed og transition — struktureret kortlægning, migrationsspor, risikovurdering	§6,stk.1, §6,stk.6	5.35, 5.36	N/A	—

Gruppe D — Segmentering

D13 — Makro-segmentering og large-scale netværk

VRF baseret tenant-isolation, multi-tenancy arkitektur og klassifikationsbaseret zoneplacering til sikring af kommuneadskillelse i stor skala. Kilde: 2.2.1 Segmentering, 2.3.1 Multi-tenancy og 2.1.1 Zoneinddeling.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Mak-1	Multi-tenancy og makrosegmentering — VRF baseret end-to-end kommuneadskillelse, GDPR-isolering	§6,stk.5	8.20, 8.22	CIS 12.2, CIS 12.6	Krav 25
Mak-2	Netværkssegmentering og tenant-isolation (DC) — dedikerede zoner pr. tenant, policy-enforcement	§6,stk.5	8.20, 8.22	CIS 12.2, CIS 12.6	Krav 25
Mak-3	Zone/segmenteringsmodel — formaliseret model med klassifikationsbaseret zoneplacering	§6,stk.5	8.20, 8.22	CIS 12.2, CIS 12.6	Krav 25
Mak-4	Klassifikationsbaseret zoneplacering — systemklassifikation afgør zone og restriktioner automatisk	§6,stk.1, §6,stk.5	5.12, 8.22	CIS 12.2, CIS 3.2	—
Mak-5	Logisk tenant-adskillelse (DC) — automatiseret håndhævelse, ressourcepools med grænser	§6,stk.4, §6,stk.5	8.22, 5.19	CIS 12.2	—
Mak-6	Kategorisering af systemer (netværksniveau) — systematisk kategorisering, sikkerheds zonetildeling	§6,stk.1	5.9, 5.12	CIS 1.1	—

D14 — Mikro-segmentering for højt kategoriserede systemer

Granulær, workload niveau segmentering med applikationsisolation, øst-vest trafikovervågning og deny-by-default. Primært til systemer med høj kritikalitet. Kilde: 2.3.1 Mikrosegmentering og 2.1.1 Zoneinddeling.

Nr.	Fokusområde	NIS2 — dansk lov (§)	ISO 27001/27002:2022	CIS Controls v8.1	Tekniske minimumskrav
Mik-1	Mikrosegmentering og sikkerhedszoner (LAN/WAN) — granulær segmentering for højt kategoriserede systemer	§6,stk.5	8.22	CIS 3.12, CIS 12.2, CIS 13.4	Krav 25
Mik-2	Netværkssegmentering på workload niveau — deny-by-default, individuelle firewall policies pr. workload	§6,stk.5	8.20, 8.22	CIS 3.12, CIS 12.2, CIS 13.4	Krav 25
Mik-3	Applikationsisolation og workload-policies — identity baserede politikker, zero trust workloads	§6,stk.5	8.22, 8.27	CIS 3.12, CIS 12.2, CIS 13.4	—
Mik-4	Firewall regelforvaltning — lifecycle-styring, versionsstyring, regelmæssige audits	§6,stk.1, §6,stk.6	8.20, 5.35	CIS 3.12, CIS 4.4/4.5, CIS 12.2, CIS 13.4	Krav 1
Mik-5	Øst-vest trafikovervågning — adfærdsbaseret anomalidetektion, realtidsanalyse intern trafik	§6,stk.2	8.16, 8.22	CIS 8.11, CIS 13.3	—
Mik-6	DNS og IPAM (platform-kontekst) — DNSSEC, centraliseret IPAM, intern/ekstern DNS adskillelse	§6,stk.1, §6,stk.5	8.20, 8.21	CIS 4.9, CIS 9.2	Krav 17, Krav 18, Krav 21, Krav 22
Mik-7	Workloads i datacenteret — mikrosegmenteret zoneplacering, eksplicit tilladelsesmodel	§6,stk.3, §6,stk.5	8.27, 8.14	CIS 3.13, CIS 12.2, CIS 13.4	—
Mik-8	Deny by default (platform niveau) — al trafik afvises som udgangspunkt, whitelist-model	§6,stk.5	8.20, 8.21	CIS 3.13, CIS 4.4/4.5, CIS 12.2, CIS 13.4	Krav 1, Krav 25

3 Referencetabel — NIS2-loven (dansk lov §§)

§§ (dansk lov)	Beskrivelse (NIS2-loven / Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau)
§7	Ledelsesansvar — ledelsesorgan godkender og fører tilsyn med cybersikkerhedsforanstaltninger; personligt ansvar og uddannelseskrav
§6,stk.1	Risikobaserede foranstaltninger og politikker for informationssystemsikkerhed (risikoanalyse og IS-politik)
§6,stk.2	Hændelseshåndtering — forebyggelse, detektion, indeslutning og genopretning
§6,stk.3	Driftskontinuitet, backup og beredskab — sikring af kritiske tjenesters tilgængelighed
§6,stk.4	Forsyningskædesikkerhed — krav til leverandørers og MSP-ers cybersikkerhed
§6,stk.5	Sikkerhed ved anskaffelse, udvikling og vedligeholdelse af net- og informationssystemer
§6,stk.6	Politikker og procedurer til vurdering af sikkerhedsforanstaltningers effektivitet
§6,stk.7	Grundlæggende cyberhygiejne og cybersikkerhedsuddannelse
§6,stk.8	Kryptografipolitikker — brug af kryptering og nøgleforvaltning
§6,stk.9	HR-sikkerhed, adgangskontrolpolitikker og aktivforvaltning
§6,stk.10	Autentifikationsløsninger (MFA), sikker kommunikation og nødkommunikationssystemer
§12	Rapporteringsforpligtelser — 24-timers indledende underretning, 72-timers rapport til CSIRT/myndighed

4 Referencetabel — ISO 27001/27002:2022

Kontrol	Titel (ISO 27002:2022)
5.1	Politikker for informationssikkerhed
5.2	Roller og ansvar for informationssikkerhed
5.9	Fortegnelse over informationer og tilknyttede aktiver
5.10	Acceptabel brug af information og andre aktiver
5.12	Klassificering af information
5.13	Mærkning af information
5.15	Adgangskontrol
5.16	Identitetsstyring
5.17	Autentifikationsoplysninger
5.18	Adgangsrettigheder
5.19	Informationssikkerhed i leverandørforhold
5.20	Håndtering af informationssikkerhed i leverandøraftaler
5.21	Styring af informationssikkerhed i IKT-forsyningskæden
5.22	Overvågning, gennemgang og ændringsstyring af leverandørydelser
5.24	Planlægning og forberedelse af hændelseshåndtering
5.25	Vurdering og beslutning om informationssikkerhedshændelser
5.26	Reaktion på informationssikkerhedshændelser
5.27	Læring af informationssikkerhedshændelser
5.29	Informationssikkerhed under forstyrrelser
5.30	IKT-parathed til forretningskontinuitet
5.31	Juridiske, lovmæssige, regulatoriske og kontraktlige krav
5.33	Beskyttelse af registreringer
5.35	Uafhængig gennemgang af informationssikkerhed
5.36	Overholdelse af politikker og standarder
5.37	Dokumenterede driftsprocedurer

Kontrol	Titel (ISO 27002:2022)
6.3	Oplysning, uddannelse og træning i informationssikkerhed
8.1	Brugerendepunktsenheder
8.2	Privilegerede adgangsrettigheder
8.3	Informationsadgangsbegrænsning
8.5	Sikker autentifikation
8.6	Kapacitetsstyring
8.8	Styring af tekniske sårbarheder
8.9	Konfigurationsstyring
8.13	Sikkerhedskopiering af information
8.14	Redundans af informationsbehandlingsfaciliteter
8.15	Logning
8.16	Overvågningsaktiviteter
8.17	Synkronisering af ure
8.19	Installation af software på driftssystemer
8.20	Netværkssikkerhed
8.21	Sikkerhed i netværkstjenester
8.22	Adskillelse af netværk
8.24	Brug af kryptografi
8.27	Sikker systemarkitektur og -ingeniørprincipper

5 Referencetabel — CIS Controls v8.1

CIS Control	Titel	IG niveau
CIS 1	Inventar og kontrol af virksomhedens aktiver	IG1
CIS 2	Inventar og kontrol af software-aktiver	IG1
CIS 3	Databeskyttelse	IG1
CIS 4	Sikker konfiguration af virksomhedsaktiver og -software	IG1
CIS 5	Kontostyring	IG1
CIS 6	Adgangsstyring	IG1
CIS 7	Kontinuerlig sårbarhedsstyring	IG2
CIS 8	Revisionslog-administration	IG2
CIS 9	E-mail- og webbrowser beskyttelse	IG2
CIS 10	Malware-forsvar	IG2
CIS 11	Gendannelse af data	IG2
CIS 12	Netværksstyring og -infrastruktur	IG2
CIS 13	Netværksovervågning og -forsvar	IG2
CIS 14	Sikkerhedsbevidsthed og færdigheder	IG2
CIS 15	Styring af tjenesteudbydere	IG2
CIS 16	Applikationssoftware-sikkerhed	IG3
CIS 17	Hændelsesrespons og -håndtering	IG3
CIS 18	Penetrationstest	IG3

6 Referencetabel — Tekniske minimumskrav

Krav	Kravformulering (Tekniske minimumskrav)
Krav 1	Der skal implementeres firewall på klienterne.
Krav 2	Klienter skal benytte Always On VPN fra eksterne netværk.
Krav 3	Fysiske klienters harddiske skal krypteres.
Krav 4	Der skal implementeres endpoint beskyttelse på klienter.
Krav 5	Klienters OS og applikationer skal holdes sikkerhedsopdateret.
Krav 6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.
Krav 7	Klienter skal anvende det nyeste operativsystem.
Krav 8	Der må kun anvendes godkendte mail-relays med autentifikation.
Krav 9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.
Krav 10	Afsenders DMARC-politik skal overholdes ved modtagelse.
Krav 11	Autentifikation til systemer over internettet skal anvende flerfaktorgodkendelse (MFA).
Krav 12	Myndigheden skal sikre, at der ikke anvendes lækkede og/eller svage passwords.
Krav 13	Anvend numerisk adgangskode på minimum seks cifre eller biometrisk identifikation på mobile enheder.
Krav 14	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.
Krav 15	OS og apps på mobile enheder skal holdes sikkerhedsopdateret.
Krav 16	Logning skal foretages på internetvendte tjenester og centrale interne it-systemer.
Krav 17	Internetvendte tjenester tilhørende myndigheden skal registreres under .dk-domæner.
Krav 18	DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.
Krav 19	Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner.
Krav 20	Der skal anvendes DANE for alle indgående mailgateways.
Krav 21	Der skal foretages validering af DNSSEC-signerede svar på navneopslag.
Krav 22	Myndigheden skal anvende en sikker DNS tjeneste eller implementere løsning til beskyttelse mod ondsindede domæner.
Krav 23	DMARC REJECT-politik implementeres på alle domæner tilhørende myndigheden.
Krav 24	Myndighedens WiFi-netværk skal være krypteret med minimum WPA2.
Krav 25	Gæstenetværk skal holdes adskilt fra myndighedens interne netværk.

Krav	Kravformulering (Tekniske minimumskrav)
Krav 26	Software på internetvendte tjenester skal holdes sikkerhedsopdateret.
Krav 27	Adgang til internetvendte tjenester skal ske over en krypteret forbindelse.
Krav 28	Internettilgængelige IP-adresser skal scannes for tjenester.
Krav 29	Software på specifikke interne infrastruktur-enheder og -tjenester skal holdes sikkerhedsopdateret.