0 Læseguide

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3

Indhold

0 Læseguide – Sådan anvendes dokumentpakken

Formål med dokumentpakken

Denne dokumentpakke udgør et samlet inspirationsmateriale, som kommende IT-Serviceorganisationer og ejerkommuner kan anvende til at understøtte arbejdet med at etablere et teknisk målbillede som fælles sigtelinje samt til at understøtte transitionen mod en samlet IT-drift og den efterfølgende transformation mod målbilledet.

Dokumenterne kan læses samlet, men er bevidst opdelt, så forskellige roller kan fokusere på de relevante dele.

1 Hoveddokumentet

Hoveddokumentet giver en strategisk indflyvning til det tekniske målbillede og etablerer et fælles narrativ på tværs af områder. Det introducerer arkitekturprincipperne og den samlede sammenhæng mellem sikkerhed, LAN/WAN, drift og compliance.

Anbefales til IT-ledere og beslutningstagere.

2 Det tekniske målbillede – fire bærende områder

Disse dokumenter udgør kernen i det tekniske målbillede. De kan læses samlet eller selektivt afhængigt af ansvar og interesse:

2.1 Teknisk målbillede – Sikkerhed

2.2 Teknisk målbillede – LAN/WAN

2.3 Teknisk målbillede – Datacenter

2.4 Teknisk målbillede – Compliance

2.4.1 Compliance_Mapping_Arkitekturprincipper

Hvert dokument beskriver:

- arkitektoniske principper
- organisatoriske forudsætninger
- sammenhæng til drift og governance

Anbefales læst af teknikere, arkitekter, driftsansvarlige og sikkerhed/compliance-roller.

3 Transition – kontrolleret overgang til fælles drift

Transitionsdokumentet beskriver, hvordan kommuner bevæger sig fra den nuværende drift til fælles drift i driftscenteret. Fokus er på:

- roller og ansvar
- snitflader mellem kommune og driftscenter
- risikohåndtering og modenhed

Anbefales læst af ledere og projektansvarlige med ansvar for implementering og overgang.

4 Transformation – varig modenhed og udvikling

Transformationsdokumentet adresserer den langsigtede udvikling efter transitionen. Her beskrives, hvordan fælles drift modnes over tid, hvordan standardisering, automatisering og governance udvikles, og hvordan driftscenteret bliver en strategisk kapabilitet.

Relevant for strategisk IT-ledelse, både centralt og i kommunerne.

5 Modenhedsvurdering

Pakke bestående af Excel-filer indeholdende scoringsmodeller og IT-serviceorganisationens mulighed for at fastsætte ambitionsniveau for sikkerhed, LAN/WAN og driftsplatform.

Relevant for it-arkitekter og teknisk personale

6 Supplerende og uddybende bilag

Følgende dokumenter bruges som reference- og arbejdsbilag og er ikke nødvendige at læse fra start, men anvendes ved behov:

- **Scorecard Servicekatalog Kommuner**
  Eksempel på scorecard til strukturering og vurdering af servicekategorier og serviceniveauer i en fælleskommunal kontekst. Indeholdte services er baseret på KL's forslag til opgavesnit vedr. Server og netværksopgave.
- **Eksempel på Onboarding checklist**
  Praktisk eksempel på en struktureret tilgang til onboarding i fælles IT-drift, der sikrer ensartet og kontrolleret overgang.

Projekt-, driftsansvarlige og IT-ledelsen

7 Versioner

Version 1.3	• Endelig version. • Denne tabel tilføjet. • 2.4.1 gennemgået og enkelte CIS henvisninger rettet. • Modenhedsanalyse ark har fået unik ID indsat for hvert punkt for lettere henvisningsmulighed. • Webinarpræsentation fra KL-webinaret den 10. juni 2026, inkluderet i dokumentpakken.
Version 1.2	• Inkl. Compliance dokument 2.4 og modenhedsanalyse. Delt bredt.
Version 1.1	• Version uden Compliance dokument 2.4 og modenhedsanalyse. Ændringer fra feedback indarbejdet. Delt begrænset.
Version 1.0	• Første version sendt til udvalgte for review og feedback.

Spørgmål til materialet bedes rettet til:
Mikael Korsgaard Juul, Projektejer i Conscia.
mj@conscia.com
+45 2516 2139

8 Begrebsfortegnelse

Begreb	Beskrivelse
802.1X	IEEE-standard for portbaseret netværksadgangskontrol.
AAA	Authentication, Authorization and Accounting; autentifikation, autorisation og sporbarhed.
Access point	Trådløst adgangspunkt til Wi-Fi-netværk.
AD	Active Directory; katalog- og identitetsplatform.
AD federering	Sammenkobling af identitetsdomæner, så identiteter kan anvendes på tværs.
AES-256	Symmetrisk krypteringsalgoritme med 256-bit nøgler.
Afhængighedskortlægning	Kortlægning af relationer mellem systemer, services, dataflows og infrastruktur.
Afvigelse	Dokumenteret forskel mellem faktisk tilstand og aftalt standard eller krav.
Aktiv/aktiv	Design hvor flere sites eller komponenter er aktive samtidig.
Aktiv/passiv	Design hvor sekundær komponent eller site står standby til failover.
Alarmering	Automatisk eller manuel varsling om hændelser, fejl eller afvigelser.
Anomalidetektion	Identifikation af afvigende adfærd eller trafikmønstre.
Any-any regel	Firewallregel der tillader bred trafik fra enhver kilde til enhver destination.
API	Application Programming Interface; grænseflade til integration og automatisering.
Arkitekturprincip	Styrende princip for designvalg, standardisering og teknisk retning.
As-is	Nuværende situation eller aktuel tilstand.
Asset management	Styring af aktiver, herunder hardware, software, systemer og livscyklus.
Asynkron replikering	Replikering hvor data kopieres med forsinkelse til sekundært site.
Audit	Uafhængig eller intern gennemgang af kontroller, processer og dokumentation.
Audit trail	Sporbar log over hvem der har gjort hvad, hvornår og med hvilken godkendelse.
authPriv	SNMPv3-sikkerhedsniveau med autentifikation og kryptering.
Backend node	Server eller serviceinstans bag en load-balancer.
Backup	Sikkerhedskopi af data, systemer eller konfigurationer.
Baseline	Godkendt standardkonfiguration eller normaltilstand.
Baselining	Etablering af normaltilstand, så afvigelser kan opdages.
Betinget adgang	Adgang der afhænger af kontekst, risiko, bruger, enhed eller lokation.
BGP	Border Gateway Protocol; routingprotokol til policy-baseret routing mellem domæner.
Blueprint	Praktisk reference eller skabelon for hvordan en måltilstand kan realiseres.

Begreb	Beskrivelse
Breach and Attack Simulation	Simuleret angrebstest til løbende validering af sikkerhedskontroller.
Bølge	Grupperet overgangsforløb hvor flere kommuner eller aktiviteter håndteres i samme strukturerede fase.
Carrier-net	Netværk leveret af tele-/netværksoperatør.
CASB	Cloud Access Security Broker; kontrol og synlighed for brug af cloudtjenester.
CEF	Common Event Format; standardiseret logformat.
CERT	Computer Emergency Response Team; team der håndterer cybersikkerhedshændelser.
Certifikatstyring	Administration af digitale certifikater, udstedelse, fornyelse og tilbagekaldelse.
Change	Kontrolleret ændring i system, infrastruktur, service eller konfiguration.
Change management	Proces for vurdering, godkendelse, implementering og dokumentation af ændringer.
Chargeback	Fordeling eller afregning af omkostninger efter faktisk forbrug.
CI/CD	Continuous Integration/Continuous Delivery; pipeline til automatiseret test og udrulning.
CIFS/SMB	Filprotokoller til deling af filer over netværk, ofte i Windows-miljøer.
CIS Benchmarks	Tekniske hardening anbefalinger for platforme, systemer og infrastrukturkomponenter.
CIS Controls	Prioriteret sæt sikkerhedskontroller fra Center for Internet Security.
CIS IG1/IG2/IG3	Implementeringsgrupper i CIS Controls, der angiver modenheds- og ambitionsniveau.
CLI	Command Line Interface; kommandolinjeadgang til systemer og netværksudstyr.
CMDB	Configuration Management Database; register over komponenter, relationer, ejerskab og kritikalitet.
Compliance	Efterlevelse af krav, standarder, politikker og regulatoriske forpligtelser.
Compute	Server- og beregningsressourcer til workloads.
Confidential Computing	Beskyttelse af data under behandling ved brug af hardwarebaseret isolation, fx sikre enclaves, ofte anvendt i multi-tenant eller højsikkerhedsmiljøer.
Configuration Item (CI)	Registreret komponent i CMDB, fx server, netværksenhed, service eller applikation.
Connectivity	Netværksforbindelse eller forbindelsesydelse mellem brugere, lokationer og services.
Container	Letvægtsruntime til applikationer isoleret fra underliggende system.
CSIRT	Computer Security Incident Response Team; formel hændelseshåndteringsfunktion, ofte national eller sektoriel.

Begreb	Beskrivelse
Curve25519	Elliptisk kurve anvendt til moderne kryptografi og nøgleudveksling.
Data at rest	Data lagret på disk, storage, backup eller arkiv.
Data in motion	Data under transport mellem systemer, lokationer eller brugere.
Data-resiliency	Dataens evne til at forblive tilgængelig, korrekt og genskabelig ved fejl.
Dataintegritet	Sikkerhed for at data er korrekte og ikke ændret utilsigtet.
Dataklassifikation	Klassificering af data efter følsomhed, forretningsværdi eller regulatorisk betydning.
DDoS	Distributed Denial of Service; angreb hvor mange kilder overbelaster en service.
Deduplikering	Reduktion af storageforbrug ved at gemme identiske data én gang.
Deny-by-default	Sikkerhedsprincip hvor trafik som udgangspunkt blokeres, medmindre den er eksplicit tilladt.
Deployment	Udrulning eller idriftsættelse af system, konfiguration eller service.
DHCP	Dynamic Host Configuration Protocol; automatisk tildeling af IP-konfiguration.
DLP	Data Loss Prevention; kontroller der reducerer risiko for datalækage.
DMZ	Demilitarized Zone; netværkszone til kontrolleret eksponering mod eksterne netværk.
DNS	Domain Name System; navneopløsning mellem navne og IP-adresser.
DNSSEC	Sikkerhedsudvidelse til DNS, der validerer integritet og ægthed af DNS-svar.
DPA	Data Processing Agreement; databehandleraftale.
DR	Disaster Recovery; genopretning efter større nedbrud eller katastrofe.
DR orkestrering	Automatiseret styring af DR-processer, fx failover og validering.
DR plan	Dokumenteret plan for genopretning af kritiske systemer og services.
Driftshåndbog	Dokumentation af driftsaftaler, procedurer, ansvar, kontakter og serviceprocesser.
Driftsplatform	Samlet teknisk platform for compute, storage, virtualisering, backup, automation og drift.
Dual power	To uafhængige strømforsyninger til kritisk udstyr.
EAP-TLS	Certifikatbaseret autentificeringsmetode til 802.1X.
eBGP	External BGP; BGP mellem forskellige administrative domæner.
EDR	Endpoint Detection and Response; detektion og respons på klienter og servere.
Emergency Change	Hasteændring der gennemføres hurtigt for at afhjælpe kritisk fejl eller risiko.
Endpoint	Slutpunkt som pc, server, mobil eller anden enhed.
Endpoint compliance	Kontrol af at en enhed lever op til sikkerhedskrav før adgang.
Event drevet orkestrering	Automatisering der udløses af hændelser eller alarmer.
Evidens	Dokumentation for at en kontrol eller proces er implementeret og virker.
EVPN	Ethernet VPN; kontrolplan ofte anvendt sammen med VXLAN.

Begreb	Beskrivelse
Exit kriterier	Kriterier der skal være opfyldt for at afslutte en fase eller aktivitet.
Failover	Skift fra primær til sekundær ressource ved fejl.
Faseopdelt model	Model hvor overgang eller udvikling opdeles i sekventielle faser.
Fileless attack	Angreb der primært udnytter hukommelse, scripts eller legitime værktøjer frem for filer.
Firewall	Sikkerhedskomponent der kontrollerer trafik mellem zoner, netværk eller systemer.
Firewall regelforvaltning	Proces for at oprette, dokumentere, reviewe og afvikle firewall-regler.
Forecasting	Fremskrivning af fremtidigt forbrug eller kapacitetsbehov.
Forsyningskædesikkerhed	Sikkerhed i relationer til leverandører, serviceorganisationer og tekniske afhængigheder.
FWaaS	Firewall as a Service; firewall funktion leveret som service.
Gap analyse	Analyse af forskel mellem as-is og ønsket måltilstand.
GDPR	EU's databeskyttelsesforordning med krav til behandling af personoplysninger.
Gendannelsesverifikation	Test eller automatisk kontrol af at data kan gendannes fra backup.
Go-live	Tidspunkt hvor en service eller driftsmodel formelt sættes i produktion.
Governance	Styringsstruktur for beslutninger, ansvar, rapportering, prioritering og opfølgning.
GPU	Graphics Processing Unit; processor til grafiske eller parallelle beregningsopgaver.
Hardening	Engelsk term for hærdning; bør som hovedregel forklares eller fordanskes.
HCI	Hyperconverged Infrastructure; samlet compute, storage og virtualisering i integreret platform.
Health monitoring	Overvågning af komponenters tilstand for at opdage fejl eller degradering.
Hidden primary	DNS-arkitektur hvor den primære zonekilde ikke er direkte eksponeret.
High Availability (HA)	Design hvor redundante komponenter reducerer risiko for nedetid.
Hypercare	Intensiv stabiliseringsperiode efter go-live med tæt opfølgning og hurtig justering.
Hypervisor	Softwarelag der kører og styrer virtuelle maskiner på fysisk hardware.
Hærdning	Sikker konfiguration af systemer ved at reducere angrebsflade og lukke svagheder.
IaC	Infrastructure as Code; Automatiseret styring af infrastruktur via kode og standardiserede skabeloner, der sikrer ensartet og skalerbar drift.
IaaS	Infrastructure as a Service; compute, storage og netværk leveret som service.
IAM	Identity and Access Management; identitets- og adgangsstyring.
IDS	Intrusion Detection System; system der opdager mistænkelig trafik.
IEEE 802.1Q	Standard for VLAN-tagging på Ethernet-netværk.

Begreb	Beskrivelse
IG	Implementation Group — implementeringsgruppe i CIS Controls (IG1-IG3)
IGP	Interior Gateway Protocol; routingprotokol internt i en organisation.
IKEv2	Internet Key Exchange version 2; protokol til nøgleudveksling i IPsec.
Immutable backup	Backup der ikke kan ændres, slettes eller manipuleres i den definerede opbevaringsperiode.
Incident	Uplanlagt hændelse eller forstyrrelse, der påvirker en IT-service.
Incident response	Proces for at opdage, analysere, inddæmme, afhjælpe og lære af hændelser.
Internet edge	Grænsepunkt mellem organisationens netværk og internet.
Internet exit	Punkt hvor organisationens trafik forlader netværket mod internet.
IoC	Indicator of Compromise; teknisk indikator på mulig kompromittering.
IP adresseplan	Plan for tildeling og strukturering af IP-adresser og subnets.
IPAM	IP Address Management; central styring af IP-adresser og subnets.
IPS	Intrusion Prevention System; system der blokerer skadelig trafik.
IPsec	Protokolsuite til kryptering og autentificering af IP-trafik.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 6.
IS-IS	Intermediate System to Intermediate System; intern routingprotokol.
ISAE 3000	Revisionsstandard for assurance på ikke-finansielle kontroller, fx informationssikkerhed og privatliv.
ISAE 3402	Revisionsstandard for kontroller hos serviceorganisationer, typisk relateret til drift og kontrolmiljø.
ISMS	Information Security Management System; ledelsessystem for informationssikkerhed.
ISO/IEC 27001	International standard for ledelsessystem for informationssikkerhed (ISMS).
ISO/IEC 27002	Kontrolkatalog med informationssikkerhedskontroller, der understøtter ISO 27001.
IT-serviceorganisation	Fælles driftsenhed, der leverer og driver kommunal IT-infrastruktur på vegne af ejerkommuner.
ITSM	IT Service Management; processer og værktøjer til styring af IT-services.
JSON	Struktureret dataformat ofte anvendt til logs og integrationer.
Just-in-time access	Tidsbegrænset tildeling af privilegeret adgang til en konkret opgave.
Kapacitetsplanlægning	Planlægning af fremtidigt behov for compute, storage, netværk og backup.
Klassifikationstaksonomi	Fælles struktur for klassificering af systemer, data og kritikalitet.
Known error	Kendt fejl med identificeret årsag og evt. workaround.
Komprimering	Reduktion af datastørrelse for at spare storagekapacitet.
Konfigurationsdrift	Afvigelser fra den godkendte standardkonfiguration over tid.
Konsekvensanalyse	Vurdering af påvirkning ved ændringer eller hændelser.

Begreb	Beskrivelse
Kontinuerlig forbedring	Løbende forbedring af processer, kontroller, drift og platform baseret på erfaringer og målinger.
Kontrolmapping	Kortlægning af krav til konkrete tekniske eller organisatoriske kontroller.
Korrigerende handlingsplan	Plan for at lukke en afvigelse eller reducere risiko.
KPI	Key Performance Indicator; målepunkt for kvalitet, drift, modenhed eller performance.
Kryptering i hvile	Kryptering af lagrede data.
Kryptering under transport	Kryptering af data, mens data sendes mellem systemer.
Kryptografisk asset management	Styring af kryptografiske nøgler, certifikater og relaterede aktiver.
Kubernetes	Orkestreringsplatform til drift af containere.
Labelling	Navngivnings-/mærkningspraksis for systemer og objekter; UK English formen er labelling.
LAN	Local Area Network; lokalt netværk på en lokation.
Lateral movement	Angribers bevægelse internt mellem systemer efter initial kompromittering.
Legacy	Ældre teknologi eller system, som ofte har begrænsninger ift. sikkerhed eller integration.
Leverandøruafhængighed	Princip om at minimere unødig binding til proprietære teknologier og bevare strategisk handlefrihed.
Lifecycle styring	Styring af et aktivs livsforløb fra etablering til udfasning.
Living-off-the-land	Angrebsteknik hvor legitime systemværktøjer misbruges.
Load balancer	Komponent der fordeler trafik på flere backend-systemer.
Logdækning	Omfanget af relevante logkilder, der er koblet til central logning.
Logkilderegister	Register over systemer og komponenter der skal levere logs.
MAB	MAC Authentication Bypass; fallback hvor enheds MAC anvendes til adgangskontrol.
MACsec	Layer 2 kryptering til Ethernet forbindelser.
Makrosegmentering	Overordnet netværksadskillelse, fx mellem kommuner, zoner eller større domæner.
Malware	Skadelig software.
Managed Service	Driftsmodel hvor en serviceorganisation har operationelt ansvar for drift og overvågning.
MDR	Managed Detection and Response; managed sikkerhedsovervågning og responsydelse.
Metadata	Strukturerede oplysninger om et objekt, fx ejer, miljø, kritikalitet og backupklasse.
MFA	Multi Factor Authentication; adgang baseret på flere faktorer.
Migration	Flytning af systemer, data eller drift fra ét miljø til et andet.
Mikrosegmentering	Finmasket segmentering på workload-, applikations- eller kommunikationsniveau.
MITRE ATT&CK	Rammeværk for kendte angrebsteknikker og taktikker.

Begreb	Beskrivelse
Modenhedsvurdering	Vurdering af kommunens aktuelle tekniske og organisatoriske parathed ift. målbilledet.
MPLS	Multiprotocol Label Switching; transportteknologi i WAN-netværk.
MSP	Managed Service Provider; organisation der leverer managed services.
mTLS	Mutual Transport Layer Security; TLS-baseret autentificering hvor både klient og server validerer hinandens certifikater, typisk anvendt til service-to-service-kommunikation i Zero Trust arkitekturer
MTTD	Mean Time To Detect; gennemsnitlig tid til at opdage en hændelse.
MTTR	Mean Time To Repair/Recover; gennemsnitlig tid til afhjælpning eller genopretning.
Multi site	Design med flere geografisk eller fysisk adskilte sites.
Multi-tenancy	Delt platform hvor flere kommuner bruger fælles infrastruktur med logisk adskillelse.
Målarkitektur	Den ønskede fremtidige tekniske tilstand, som kommuner og IT-Serviceorganisation gradvist bevæger sig imod.
NaaS	Network as a Service; netværk leveret som standardiseret managed service.
NAC	Network Access Control; kontrol af hvilke enheder der må få adgang til netværket.
NAS	Network Attached Storage; filbaseret storage over netværk.
NETCONF	Standardiseret protokol til konfiguration af netværksudstyr.
NFS	Network File System; protokol til filbaseret storageadgang.
NIS2	EU-direktiv om net- og informationssikkerhed med krav til risikostyring, ledelsesansvar, forsyningskæde og hændelsesrapportering.
NIS2 Artikel 20	Bestemmelse om ledelsesansvar og ledelsens rolle i cybersikkerhed.
NIS2 Artikel 21	Bestemmelse om risikostyringsforanstaltninger, herunder backup, adgang, kryptografi, forsyningskæde og hændelseshåndtering.
NIS2 Artikel 23	Bestemmelse om rapportering af væsentlige hændelser.
NOC	Network Operations Center; funktion for overvågning og drift af netværk og infrastruktur.
Nord-syd trafik	Trafik ind og ud af et miljø, fx mellem datacenter og internet.
Normal Change	Ændring der kræver vurdering og godkendelse før implementering.
NSP	Network Service Provider; netværksoperatør/carrier.
NTP	Network Time Protocol; protokol til tidsynkronisering.
NTS	Network Time Security; sikker udvidelse til NTP.
NVMe	Non-Volatile Memory Express; højtydende storageinterface/protokol.
Nøglehåndtering	Administration af kryptografiske nøgler gennem deres livscyklus.
Offboarding	Kontrolleret afvikling og oprydning ved udtræden eller fjernelse af en tenant/service.
Onboarding	Kontrolleret indførsel af en kommune, tenant, service eller workload i fælles drift.

Begreb	Beskrivelse
Opgavesnit	Afgrænsning af hvilke opgaver og ansvar der ligger hos henholdsvis kommune og IT-serviceorganisation.
OIDC	OpenID Connect; identitets- og autentifikationsprotokol baseret på OAuth 2.0, anvendt til moderne federeret login og integrationsscenarier.
OpenTelemetry	Åben standard til indsamling og eksport af metrics, logs og traces fra applikationer og platforme, anvendt til driftsovervågning, performanceanalyse og sikkerhed.
OSPF	Open Shortest Path First; åben intern routingprotokol.
Overallokering	Tildeling af flere ressourcer end et workload reelt har behov for.
PaaS	Platform as a Service; middleware, database eller containerplatform leveret som service.
Passkeys	Password fri autentificeringsmetode baseret på kryptografiske nøgler bundet til enheder eller brugerkonti, designet til at være phishing resistent
PAM	Privileged Access Management; styring af privilegerede administrative adgange.
Patch management	Proces for identifikation, prioritering, test og installation af opdateringer.
PAW	Privileged Access Workstation; særskilt sikret arbejdsstation til administrative opgaver.
Penetrationstest	Kontrolleret test af sikkerhed ved at forsøge at udnytte sårbarheder.
Pipeline	Automatiseret kæde af trin for validering, godkendelse og udrulning.
PKI	Public Key Infrastructure; infrastruktur til certifikater og nøglestyring.
Playbook	Struktureret handlingsforløb for hændelser eller DR-scenarier.
Policing	Håndhævelse af trafikgrænser ved at begrænse eller droppe trafik.
Policy-as-code	Politikker defineret og håndhævet som kode.
Posture assessment	Vurdering af en enheds sikkerhedstilstand før eller under adgang.
Post-Quantum Cryptography (PQC)	Kryptografiske algoritmer designet til at modstå angreb fra kvantecomputere; relevant i langsigtet arkitektur- og kryptoplanlægning.
Predictive failure analysis	Analyse der forsøger at forudsige komponentfejl før de indtræffer.
Problem	Underliggende årsag til én eller flere incidents.
Producentagnostisk	Beskrivelse af principper der ikke forudsætter en bestemt producent eller teknologi.
Provisionering	Oprettelse og tildeling af tekniske ressourcer som VM, storage, netværk eller adgang.
Purple team	Samarbejde mellem offensive og defensive sikkerhedsroller for at validere og forbedre kontroller.
QoS	Quality of Service; prioritering og styring af trafik for at sikre kvalitet.

Begreb	Beskrivelse
Quorum	Mekanisme der afgør hvilken del af et distribueret system der må fortsætte drift ved opdeling.
RACI	Ansvarsmodel: Responsible, Accountable, Consulted og Informed.
RADIUS	Protokol/serverfunktion til central autentifikation og autorisation af netværksadgang.
Ransomware	Skadelig software der krypterer eller blokerer adgang til data mod krav om betaling.
RBAC	Role-Based Access Control; adgangsstyring baseret på roller.
RBI	Remote Browser Isolation; isolering af webbrowsing i separat miljø.
Recovery	Genopretning af systemer, services eller data efter fejl eller hændelse.
Remediation	Korrigerende handling, manuel eller automatisk, der lukker en afvigelse.
Request fulfilment	Proces for behandling og levering af service requests.
RESTCONF	REST-baseret protokol til konfiguration og management af netværksudstyr.
Restore	Gendannelse af data eller systemer fra backup.
Retention	Periode hvor data, logs eller backup opbevares.
RFC 1918	Private IPv4 adresserum til intern brug.
RFC 5424	Standard for struktureret syslog-format.
Rightsizing	Tilpasning af ressourcer til faktisk behov for at undgå over- eller underallokering.
Risikoaccept	Formel beslutning om at acceptere en kendt risiko.
Risikoregister	Register over identificerede risici, ejere, vurderinger og håndtering.
Roadmap	Faseopdelt plan for udvikling eller implementering over tid.
Root cause	Grundlæggende årsag til en hændelse eller fejl.
Router	Netværkskomponent der videresender trafik mellem netværk baseret på routing.
Routing	Videresendelse af trafik mellem netværk.
RPO	Recovery Point Objective; maksimalt acceptabelt datatab målt i tid.
RTO	Recovery Time Objective; maksimalt acceptabel tid til genopretning af en service.
Runbook	Dokumenteret driftsprocedure for en gentagelig opgave eller hændelse.
SAN	Storage Area Network; netværksbaseret blokstorage.
SASE	Secure Access Service Edge; samling af netværks- og sikkerhedsfunktioner som cloudbaseret arkitektur.
SATA	Serial ATA; storageinterface ofte anvendt til kapacitetslag.
SBOM	Software Bill of Materials; struktureret oversigt over softwarekomponenter, afhængigheder og versioner, anvendt til forsyningskædesikkerhed, sårbarhedsstyring og risikovurdering
Scorecard	Struktureret vurderingsskema, hvor målepunkter scores mod definerede modenhedsniveauer.

Begreb	Beskrivelse
SD WAN	Software Defined WAN; softwarestyret WAN med central orkestrering.
Self healing	Automatiseret genopretning af kendte fejltilstande.
Self-service	Mulighed for at rekvirere standardydelser via portal eller workflow uden manuel specialbehandling.
Service Request	Anmodning om standardiseret service eller ydelse.
Service Review	Periodisk gennemgang af servicekvalitet, hændelser, forbedringer og aftalte mål.
Serviceeksponering	I hvilket omfang en service er tilgængelig internt, eksternt eller på internet.
Servicekatalog	Katalog over standardiserede ydelser, serviceniveauer og leverancer.
Showback	Synliggørelse af forbrug og omkostninger uden egentlig afregning.
SIEM	Security Information and Event Management; platform til indsamling, korrelation og analyse af sikkerhedslogs.
SIGMA regler	Standardiseret, platformuafhængigt format til beskrivelse af detektionsregler, der kan oversættes til konkrete SIEM regler på tværs af leverandører.
Sikkerhedseffektivitet	Hvor effektivt en kontrol faktisk reducerer risiko i praksis.
Sikkerhedszone	Logisk afgrænset område med fælles sikkerhedspolitik.
SLA	Service Level Agreement; aftalt serviceniveau, fx oppetid, svartid eller tilgængelighed.
SLO	Service Level Objective; målsætning for servicekvalitet eller driftsmål.
Snapshot	Punkt-i-tid-kopi af data eller systemtilstand.
SNMP	Simple Network Management Protocol; protokol til overvågning og management af enheder.
SNMPv1/v2c	Ældre SNMP-versioner med begrænset sikkerhed.
SNMPv3	Sikrere SNMP-version med autentifikation og kryptering.
SOAR	Security Orchestration, Automation and Response; automatisering af sikkerhedsrespons og arbejdsgange.
SOC	Security Operations Center; funktion for sikkerhedsovervågning, analyse og respons.
SOC 2 Type II	Assurance rapport om sikkerhed, tilgængelighed, fortrolighed m.v. over en periode.
Split-brain	Fejltilstand hvor flere systemdele tror, de er primære samtidig.
Split-horizon DNS	DNS-design hvor interne og eksterne klienter får forskellige DNS-svar.
SSD	Solid State Drive; hurtig lagringsteknologi uden roterende medier.
SSH	Secure Shell; krypteret protokol til administrativ adgang.
SSHv2	Version 2 af SSH-protokollen.
Stabilisering	Periode hvor drift justeres og fejl rettes efter overdragelse eller go-live.
Standard Change	Forhåndsgodkendt, lavrisikoændring med kendt procedure.
Storage	Lagringsressourcer til data, virtuelle maskiner, backup og applikationer.

Begreb	Beskrivelse
Storage tiering	Placering af data på forskellige lag efter performance, kapacitet eller kritikalitet.
Subnet	Delnet inden for et IP adresserum.
Supernet	Større IP-adresseblok der kan opdeles i mindre subnets.
SWG	Secure Web Gateway; sikkerhedskontrol for webtrafik.
Switch	Netværkskomponent der forbinder enheder i et LAN.
Synkron replikering	Replikering hvor data skrives til flere steder samtidig før skrivning bekræftes.
Syslog	Standardprotokol til transport af logbeskeder.
Systemkritikalitet	Vurdering af hvor kritisk et system er for forretning, drift eller samfundsopgaver.
Sårbarhedsstyring	Løbende identifikation, vurdering og håndtering af tekniske sårbarheder.
Tagging	Tildeling af metadata til objekter for at understøtte styring, rapportering og automatisering.
Teknisk målbillede	Fælles arkitektonisk retning, principper og anbefalede modenhedsniveauer for fælleskommunal IT-drift.
Tekniske minimumskrav	Fælles eller statslige tekniske krav til sikkerhed, logning, kryptering, adgang m.v.
Telemetri	Måle- og hændelsesdata fra systemer, netværk, endpoints og cloud.
Telemetri pipeline	Kæde for indsamling, transport, normalisering og routing af telemetri/logs.
Telnet	Ældre ukrypteret fjernadgangsprotokol.
Tenant	Logisk adskilt enhed eller kundeområde på en fælles platform.
Tenant isolation	Teknisk og logisk adskillelse mellem tenants.
Thin provisioning	Storage-teknik hvor kapacitet tildeles logisk før den fysisk forbruges.
Threat Intelligence	Trusselsinformation om aktører, metoder, indikatorer og aktuelle sårbarheder.
TLS	Transport Layer Security; krypteret transportprotokol.
TLS 1.2+	Minimumsniveau for moderne krypteret transport i materialet.
To-be	Ønsket fremtidig tilstand.
Traffic shaping	Kontrol af trafikmængder og båndbredde for at styre belastning.
Transformation	Langsigtet udvikling efter transition, hvor drift, sikkerhed, platforme og processer modnes over tid.
Transition	Kontrolleret overgang fra nuværende kommunal drift til fælles drift i IT-serviceorganisationen.
Tredjepartsrevision	Revision udført af uafhængig part.
TTP	Tactics, Techniques and Procedures; angriberes fremgangsmåder.
Tuning	Tilpasning af regler og alarmer for at reducere støj og øge præcision.
UDP-syslog	Syslog over UDP; ofte ukrypteret og uden leveringsgaranti.
UPS	Uninterruptible Power Supply; nødstrømsforsyning ved strømsvigt.
UTC stempling	Brug af fælles tidsreference i logs og hændelser.
Virtualisering	Teknologi hvor fysiske ressourcer opdeles i virtuelle servere eller miljøer.

Begreb	Beskrivelse
VLAN	Virtual LAN; logisk opdeling af et fysisk netværk.
VM	Virtuel maskine; softwarebaseret servermiljø.
VM skabelon	Standardiseret, hærdet skabelon til oprettelse af virtuelle maskiner.
VNI	VXLAN Network Identifier; segment-id i VXLAN.
VPN	Virtual Private Network; krypteret eller logisk tunnel mellem netværk eller brugere.
VRF	Virtual Routing and Forwarding; separate routingtabeller til logisk netværksadskillelse.
VXLAN	Virtual Extensible LAN; overlay teknologi til skalerbar netværkssegmentering.
WAN	Wide Area Network; netværk mellem lokationer, datacentre og driftsenheder.
Webfiltrering	Kontrol af webtrafik for at blokere skadelige eller uønskede destinationer.
Witness site	Tredje lokation eller funktion der understøtter quorum beslutninger i et multi-site design.
Workaround	Midlertidig løsning der reducerer effekt af en fejl uden at fjerne årsagen.
Workload	En applikation, service eller teknisk belastning, der kører på platformen.
x86	Processorarkitektur udbredt i standardservere.
XDR	Extended Detection and Response; korreleret detektion og respons på tværs af endpoints, netværk, identitet og cloud.
Zero-day	Sårbarhed eller angreb der endnu ikke har kendt rettelse eller signatur.
Zombie VM	Inaktiv eller glemt virtuel maskine, der fortsat bruger ressourcer.
Zonemodel	Struktur for inddeling af netværk og systemer i sikkerhedszoner.
ZTNA	Zero Trust Network Access; adgangsmodel hvor adgang gives ud fra identitet, kontekst og løbende verifikation.
Øst-vest trafik	Intern trafik mellem systemer eller workloads i samme miljø eller datacenter.

9 Litteraturliste

1. KLs anbefalinger til tekniske minimumskrav i kommunerne: Anbefalinger tekniske minimumskrav i kommunerne 2024_Version PDF (2025)
2. Statens minimumskrav: https://www.sikkerdigital.dk/Media/638931901863386001/De%20tekniske%20minimumskrav%202024%20opdateret%20september%202025.pdf
3. Vejledning til statens minimumskrav: https://www.sikkerdigital.dk/Media/638931901870547002/Vejledning%20til%20de%20tekniske%20minimumskrav%20-%20september%202025.pdf
4. Cyberforsvar der virker: https://samsik.dk/wp-content/uploads/2025/09/vejledning-cyberforsvar-der-virker-2023.pdf
5. Logningsbekendgørelsen: https://www.retsinformation.dk/eli/lta/2006/988
6. Gartners guide til Telemetry pipeline: https://www.gartner.com/en/documents/6906466
7. Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven): https://www.retsinformation.dk/eli/lta/2025/434
8. EUs PQC roadmap: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
9. NIST zero-trust architecture framework: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
10. Strategi for forsyningssikkerhed: https://sfos.dk/wp-content/uploads/2023/09/Strategi-for-forsyningssikkerhed.pdf
11. Cybertruslen mod danmark: https://samsik.dk/wp-content/uploads/2025/11/Cybertruslen-mod-Danmark-2025.pdf
12. NIST SP 800-215, Guide to a Secure Enterprise Network Landscape: https://csrc.nist.gov/pubs/sp/800/215/final
13. ITIL 4: Configuration Management Database (CMDB); https://www.axelos.com/certifications/itil-service-management
14. Infrastructure as Code (IaC) — NIST SP 800-204C, Implementation of DevSecOps for a Microservices-based Application with Service Mesh: https://csrc.nist.gov/pubs/sp/800/204/c/final
15. NIST SP 800-125B, Secure Virtual Network Configuration for VM Protection: https://csrc.nist.gov/pubs/sp/800/125/b/final
16. NIST SP 800-125, Guide to Security for Full Virtualization Technologies: https://csrc.nist.gov/pubs/sp/800/125/final
17. The Open Group, Cloud Computing Reference Architecture: https://www.opengroup.org/cloud-computing
18. CIS Benchmarks — Center for Internet Security: https://www.cisecurity.org/cis-benchmarks
19. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
20. NIST SP 800-63-4, Digital Identity Guidelines: https://csrc.nist.gov/pubs/sp/800/63/4/final
21. Uptime Institute, Tier Classification System: https://uptimeinstitute.com/tiers

22. ISO 22301:2019, Business Continuity Management Systems: https://www.iso.org/standard/75106.html
23. NIST SP 800-184, Guide for Cybersecurity Event Recovery: https://csrc.nist.gov/pubs/sp/800/184/final
24. NIST Cybersecurity Framework 2.0 (Recover function): https://www.nist.gov/cyberframework
25. NIST SP 800-61 Rev. 3, Computer Security Incident Handling Guide: SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | CSRC
26. MITRE ATT&CK Framework (lateral movement, threat detection): https://attack.mitre.org
27. Gartner, "Predicts 2026: AI Agents Will Transform IT Infrastructure and Operations", Cameron Haight et al., 4. december 2025: https://www.gartner.com/en/documents/7242030
28. StackGen, AI-driven infrastructure generation: https://www.stackgen.com
29. ISO 27001:2022: https://www.iso.org/standard/27001
30. ISO 27002:2022: https://www.iso.org/standard/75652.html
31. CIS v8.1 guide: https://www.cisecurity.org/controls/v8-1
32. ENISA Technical Implementation Guidance: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
33. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32022L2555&qid=1779871132732
34. NIS 2-vejledninger fra Styrelsen for Samfundssikkerhed: https://samsik.dk/nis2/nis-2-vejledninger/
35. Vejledning til kommuner om NIS 2-loven: https://samsik.dk/wp-content/uploads/2025/07/Vejledning-til-kommuner-om-NIS-2-loven.pdf
36. Google Cloud — A Practical Guide to Cloud Migration: https://sre.google/static/pdf/practical-guide-to-cloud-migration.pdf
37. Deloitte UK — Shared Services Handbook: Hit the road: https://www.deloitte.co.uk/makeconnections/assets/pdf/shared-services-handbook-hit-the-road.pdf
38. AWS – Strategy and best practises for AWS large migrations: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/strategy-large-scale-migrations/strategy-large-scale-migrations.pdf