NIS 2

Fra kompleks lovgivning til konkret handling

Janni Lee Bang Brodersen,
Informationssikkerhedschef (CISO) på SDU
Leder af Governance, Risk & Compliance SDU IT

Agenda

SDU Digital

NIS 2

Formål og betydning for universiteterne

SDU

SDU IT

Krav til foranstaltninger

SDU

SDU IT

Meningsfuld Implementering

SDU

SDU IT

IT-sikkerheds strategi

SDU

SDU IT

NIS2 implementering

SDU

SDU IT

Spørgsmål?

SDU

SDU Digital

sdu.dk

#sdudk

NIS 2

Formål og betydning for universiteterne

SDU

NIS 2 - Formål

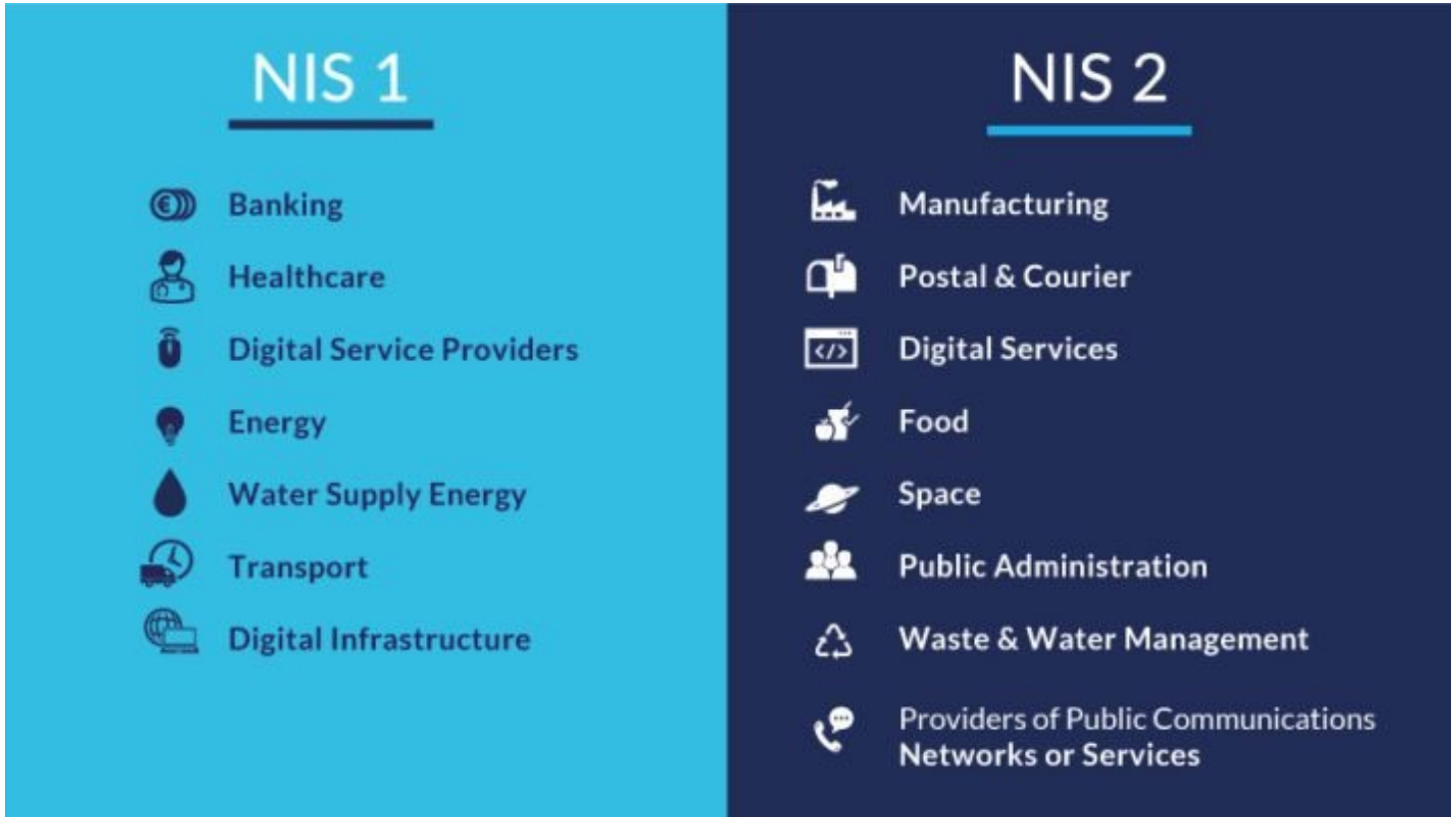
→ Styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU

→ Gælder for virksomheder indenfor en lang række sektorer og for offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet

→ krav om sikkerhedsforanstaltninger og underretning om hændelser

→ Skærpet ledelsesansvar (og dog…)

→ Skærper sanktioner og harmoniserer medlemsstaternes tilsynskompetencer og tilsynsforpligtelser



https://www.riskcrew.com/nis-2-timeline-requirements-to-minimise-risks/

Den danske implementeringsmodel

Hvem er omfattet?

Væsentlige enheder	Branche	Virksomhedstyper
	Digital infrastruktur	DNS, data centre, cloud-udbydere, MSP'er, kommunikationsplatforme, mv.
	Energi	Leverandører, distributører, udsendelse og salg af elektricitet, olie, gas, fjernvarme/køling, hydrogen, elbils ladestandsproducenter
	Transport	Luft, spor, vej- og vandtransportsvirksomheder samt fragt og havnevirksomheder. Transport omfatter både mennesker og varer.
	Offentlig forvaltning	Centraladministration og regional administration og muligvis den kommunale forvaltning*
	Bank- & finansiel markedsinfrastrukturer	Bank-, kredit-, handel- og børsvirksomheder samt deres infrastruktur.
	Sundhed	Sundhedsudbydere, forskningslaboratorier i sundhedsfremme, farmaceutiske virksomheder samt producenter af medicinal udstyr.
	Drikke- og spildevand	Drikke- og spildevandsanlæg
	Rummet	Virksomheder, der arbejder med rumfartsinfrastruktur.

Vigtige enheder	Branche	Virksomhedstyper
	Kemikalier	Virksomheder, der arbejder med fremstilling, produktion og/eller distribution af kemikalier
	Affaldshåndtering	Virksomheder, der varetager affaldshåndtering som deres primære økonomiske aktivitet.
	Post- og kurervirksomhed	Postbefordrende virksomheder samt udbydere af kurertjenester.
	Fødevarevirksomheder	Fødevarevirksomheder, der beskæftiger sig med engrosdistribution og industriel produktion og tilvirkning.
	Digitale serviceudbydere	Udbydere af onlinemarkedspladser, søgemaskiner og sociale netværkstjenester.
	Forskning	Forskningsorganisationer
	Produktionsvirksomheder af særlig vigtigt udstyr	Virksomheder, der fremstiller medicinal- og diagnoseudstyr, elektronik komponenter, maskin- og transportudstyr, reservedele, mv., der vurderes at være særligt vigtigt for samfundet.

Forskningsorganisation
En enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. Indbefatter ikke uddannelsesinstitutioner.

https://www.danskindustri.dk/vi-radgiver-dig/virksomhedsregler-og-varktojer/nis2-vejledningsunivers/hvem-er-omfattet2/

Væsentlig enheder - størrelseskrav

Væsentlige enheder	Branche
	Digital infrastruktur
	Energi
	Transport
	Offentlig forvaltning
	Bank- & finansiel markedsinfrastrukturer
	Sundhed
	Drikke- og spildevand
	Rummet

- → §4 Enheder af en type omfattet af lovens bilag 1 anses for at være væsentlige enheder, hvis enheden opfylder én af følgende betingelser.[…]
  - → 1. enheden beskæftiger 250 personer eller derover
  - → 2. enheden har en årlig omsætning på over 50 mio. euro og en årlig samlet balance på over 43 mio. euro.

- → Hvis du er en virksomhed med over 250 medarbejdere, der yder datacentertjenester er du omfattet af NIS 2, uagtet om de virksomheder man yder tjenesten til er indenfor væsentlige eller vigtige sektorer. Der er ikke krav om at aktiviteten skal understøtte samfundskritiske funktioner

- → Hvis du understøtter kritiske samfundsmæssige eller økonomiske aktiviteter er der ingen størrelseskrav – du er omfattet (gælder både væsentlige og vigtige sektorer)

Vigtige enheder - størrelseskrav

Vigtige enheder	Branche
	Kemikalier
	Affaldshåndtering
	Post- og kurervirksomhed
	Fødevarevirksomheder
	Digitale serviceudbydere
	Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr

→ § 5 Enheder af en type, som er omfattet af lovens bilag 1 eller 2, anses for at være vigtige enheder, hvis enheden ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4, og enheden opfylder mindst én af følgende betingelser:

- → Enheden beskæftiger 50 personer eller derover
- → Enheden har en årlig omsætning på over 10 mio. euro og en årlig samlet balance på over 10 mio. euro.

Stk. 2 Den kompetente myndighed kan træffe afgørelse om , at en enhed uanset størrelse, som er omfattet […] skal anses for at være en vigtig enhed.

Dvs. en væsentlig enhed, der ikke opfylder størrelseskravet på 250 for at være ”væsentlig”, men som har 60 medarbejdere bliver efter § 5 betragtet som en ”vigtig enhed”

Undtagelser

→ § 1, stk. 7 Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler om, at loven helt eller delvis også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

→ Bemærkninger til loven afsnit 2.1.3. […] *"Det er dog Ministeriet for samfundssikkerhed og beredskabs opfattelse, at offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner, der leverer tjenester inden for sektorerne i lovens bilag 1 eller 2, vil blive underlagt lovens krav. […]"*.

→ Betyder: Universiteterne bliver fuldt omfattet hvis de har specifikke aktiviteter uanset om sektoren ikke direkte omfattes

→ Præambel 88: *"[…] Navnlig bør disse enheder træffe passende foranstaltninger til at sikre, at deres samarbejde med akademiske institutioner og forskningsinstitutioner finder sted i overensstemmelse med deres cybersikkerhedspolitikker og følger god praksis med hensyn til sikker adgang til og formidling af oplysninger generelt og beskyttelse af intellektuel ejendom i særdeleshed"*.

→ Betyder: Universiteter der ikke er direkte omfattet bliver indirekte omfattet

Konkrete eksempler på aktiviteter på SDU, der vurderes at være direkte omfattet

- → Datacentertjeneste
  - → En tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central opbevaring, sammenkobling og drift af it- og netværksudstyr, der leverer datalagrings-, databehandlings- og datatransporttjenester, samt alle faciliteter og infrastruktur til energidistribution og miljøkontrol. (NIS 2-loven § 3, stk. 1, nr. 5)

- → Cloudcomputingtjenester
  - → En digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og fleksibel pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter. (NIS 2-loven § 3, stk. 1, nr. 2)

- → Forsknings- og udviklingsaktiviteter vedrørende lægemidler til mennesker

- → Myndighedsbetjening (offentlig forvaltning – måske ikke)
  - → Retsmedicinske ydelser, retskemiske ydelser, obduktioner m.fl. (ydelser i forbindelse med efterforskninger er undtaget)
  - → Evaluering af effekt af lægemidler, forskning vedr. organisering af sundhedsvæsnet, analyser af sundhedsydelser
  - → Statens Institut for Folkesundhed (SIF) har en rammeaftale med Indenrigs- og Sundhedsministeriet om myndighedsbetjening på folkesundhedsområdet, bidrag til besvarelse af §20-spørgsmål, bidrag til politiske initiativer, monitorering af folkesundheden (sundhedsprofiler og lignende)

- → Operatør af ladestationer (nok ikke)
  - → ansvarlig for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne.

Risikobaseret tilgang – og et par definitioner

→ Bemærkninger til loven: Der henvises til NIS 2-direktivets præambelbetragtning nr. 82, hvoraf det følger*, at "foranstaltninger til styring af cybersikkerhedsrisici bør stå i et* ***passende*** *forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse vil have*.

→ Præambel 82: […] *enhedens størrelse og sandsynligheden for hændelser og deres alvor* […]"

→ **Cyberhygiejnepolitikker**: Politikker for software- og hardwareopdateringer, ændringer af passwords, styring af nye installeringer (change management), begrænsning af administrative rettigheder og backup af data, beredskab og håndtering af hændelser og trusler (præambel 49)

→ **Cyberhygiejnepraksisser**: Zerotrust-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring, awarensstræning af personale (præambel 89)

→ **Hændelse**: En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare. (NIS 2-loven §3, stk. 1, nr. 12)

Krav til foranstaltninger

Krav til foranstaltninger

NIS 2-loven § 6 (art. 21 NIS 2-direktiv)

→ § 6 Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte følgende:

- → 1. Politikker for risikoanalyse og informationssystemsikkerhed
- → 2. Håndtering af hændelser
- → 3. Drifskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.
- → 4. Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.
- → 5. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
- → 6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
- → 7. Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
- → 8. Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering
- → 9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
- → 10. Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant

Dvs. man er godt med, hvis man arbejder efter ISO 27001/2

Fra soft law til ”rigtig” lov

Kommissionens gennemførelsesforordning – gælder bl.a. datacentertjenester og cloudcomputingtjenester

Politik for sikkerheden i net- og informationssystemer
→ Roller, ansvarsområder og bemyndigelser
Rammer for risikostyring
→ Overvågning af overholdelse
Politik for håndtering af hændelser
→ Overvågning og logning
→ Indberetning af begivenheder
→ Vurdering og klassifikation af begivenheder
→ Reaktion på hændelser, Gennemgang efter hændelser
Driftskontinuitets- og katastrofeplan
→ Styring af backups og reserver
→ Krisestyring
Politik for forsyningskædesikkerhed
→ Fortegnelse over leverandører og tjenesteydere
Sikkerhed i forbindelse med erhvervelse af IKT-tjenester eller IKT-produkter
→ Sikker udviklingsproces, Konfigurationsstyring
→ Ændringsstyring, reparation og vedligeholdelse
→ Sikkerhedstest, Sikkerhedspatchstyring
→ Netsikkerhed, Netsegmentering
→ Beskyttelse mod skadelig og uautoriseret software
→ Håndtering og offentliggørelse af sårbarheder

Bevidstgørelse og grundlæggende cyberhygiejnepraksisser
→ Sikkerhedsuddannelse
Kryptografi
Personalesikkerhed
→ Baggrundskontrol
→ Procedurer ved ophør eller ændring af ansættelsesforhold
→ Disciplinærprocedure
Politik for adgangskontrol
→ Forvaltning af adgangsrettigheder
→ Privilegerede konti og systemadministrationskonti
→ Administrationssystemer
→ Identifikation, Autentificering, Multifaktor-autentificering
Klassifikation af aktiver
→ Håndtering af aktiver
→ Politik om mobile enheder
→ Fortegnelse over aktiver
Miljømæssig og fysisk sikkerhed
→ Understøttende forsyningstjenester
→ Beskyttelse mod fysiske og miljømæssige trusler
→ Perimeterkontrol og fysisk adgangskontrol

Kommer til at smitte af på fortolkningen af ”passende tekniske og organisatoriske foranstaltninger”

Opsummering

Væsentlige enheder	Branche
	Digital infrastruktur
	Energi
	Transport
	Offentlig forvaltning
	Bank- & finansiel markedsinfrastrukturer
	Sundhed
	Drikke- og spildevand
	Rummet

Vigtige enheder	Branche
	Kemikalier
	Affaldshåndtering
	Post- og kurervirksomhed
	Fødevarevirksomheder
	Digitale serviceudbydere
	Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr

- → Træder i kraft d. 1. juli 2025
- → Universiteterne omfattet hvis særlige aktiviteter
- → Risikobaseret tilgang
  - → Start med det der ville være direkte omfattet
- → Foranstaltninger som vi kender fra ISO 27001/2
  - → Nu med lidt flere konkrete krav
- → Krav til uddannelse af ledelse og medarbejdere
- → Krav om rapportering af hændelser
- → Risiko for bøder, 2% (10 mio. euro) eller 1,4% (7 mio. euro)
- → Ledelsen (bestyrelse, direktion)
  - → Passende forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden
  - → Føre tilsyn med foranstaltningernes gennemførelse

Vejledninger

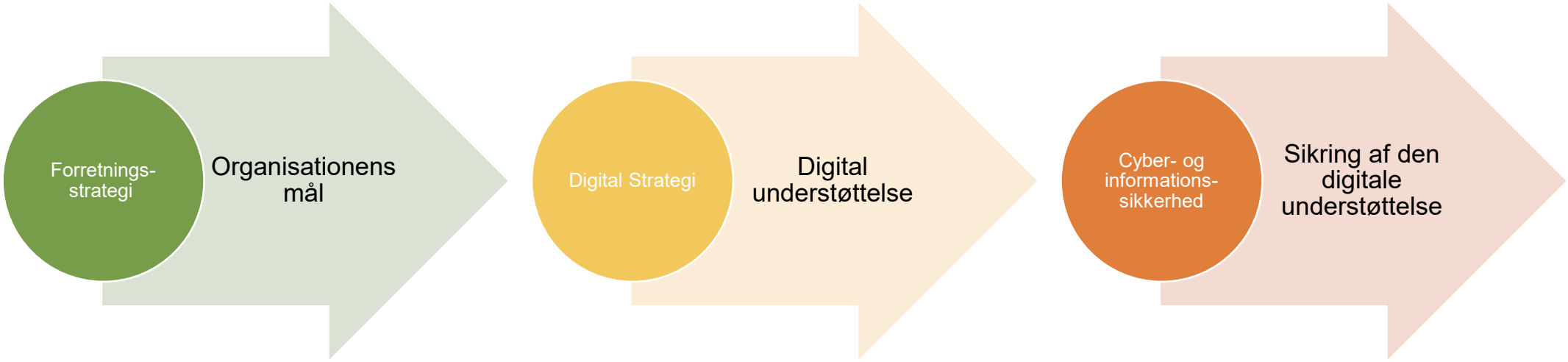
https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Vejledninger - SAMSIK

https://samsik.dk/nis2/nis-2-vejledninger/

Meningsfuld Implementering

Sammenhæng mellem strategier



Figur lavet på baggrund af ”Cybersikkerhed – helt sikkert”, 2024

- → Forstå organisationens overordnede strategiske retning og mål
- → Afstem ledelsens risikoappetit.
  - → Hvilke risici og konsekvenser kan organisationen ikke leve med?
- → Hvilke kerneprocesser understøtter målopnåelsen
  - → Identificer særligt vigtige forretningsområder eller processer fx forskning, undervisning, studieoptag… osv.
- → Hvilken digital understøttelse er der af processerne?
- → Dokumenter IT-understøttelsen
  - → Hvilke systemer, data og infrastrukturkomponenter støtter opgaveløsningen i forretningsprocesserne?

Få styr på Governance

Indsigt og prioriteringer

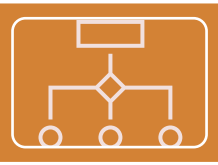
- Identificer områder hvor der skal arbejdes med cyber- og informationssikkerhed i form af processer eller investeringer
- Afdækning af risikoappetit med ledelsen og tilpas risikostyringen

Lovgivning, standarder og politikker

- Få klarhed over, hvilke krav der er til organisationen (lovgivning, standarder, politiker)
- Validering af overholdelse af krav samt rapportering heraf (er der behov for ekstern audit/tilsyn?)

Risikostyring (sæt ind, hvor værdien er størst)

- Prioriter de vigtigste risici først
- Tydelig ansvarsfordeling i organisationens risikostyring



Roller og ansvar (hvem kan tage beslutninger om hvad?)

- Opbygning af klar governance (styringsmodel) på tværs af organisationen
- Ledelsen understøtter arbejdet med ressourcer og kan oversætte arbejdet til organisatorisk kontekst

It-beredskab og håndtering af krisesituationer

- Forretningskontinuitet (business continuitet) bygger på en solid forståelse for organisationens kerneprocesser
- Udarbejdelse af beredskabet kan følge plan-do-check-act-metoden for at sikre løbende evaluering og opdatering

Awareness og adfærdsdesign

- Løfte medarbejdernes generelle sikkerhedsniveau i organisationen
- Medarbejderne skal kende truslerne og deres ansvar i den forbindelse

Figur lavet på baggrund af Cybersikkerhed – helt sikkert, 2024

Få styr på Governance

Tjekliste:

→ Er organisationens vigtigste arbejdsprocesser kortlagt?
→ Er viden om forretningsmæssig kritikalitet omsat til sikkerhedstiltag, der effektivt beskytter eller opretholder opgavevaretagelsen?
→ Er der klarhed over ledelsens risikoappetit?

→ Understøtter ledelsen med sin prioritering af medarbejderressourcer de aktuelle lovkrav, rapporterings- og opfølgningsforpligtelser, som organisationen er omfattet af?
→ Har organisationen besluttet hvordan lovkrav skal efterleves?

→ Har ledelsen forståelse for de risici, som organisationen står overfor?
→ Har ledelsen godkendt risikotærskel samt mitigerende handlinger?

Figur lavet på baggrund af Cybersikkerhed – helt sikkert, 2024

Få styr på Governance

Tjekliste:

→ Har organisationen en tydelig governance (styringsmodel) for cyber- og informationssikkerhed?

→ Hvordan sikrer organisationen at have de rette kompetencer blandt medarbejder til at kunne løfte de prioriterede opgaver?

→ Ved organisationen, hvem der skal træde til i tilfælde af en krise, og hvad de har mandat til at gøre?

→ Hvilke forretningsprocesser skal have fokus først i en krisesituation, og hvordan kan de opretholdes uden den normale IT-understøttelse?

→ Har organisationen en tydelig kommunikationsplan, der kan følges i en krisesituation?

→ Har organisationen blik for, at undervisning eller kommunikationskampagner ofte ikke i sig selv er nok for at sikre reel adfærdsændring?

→ Hvordan kan nye sikkerhedsforanstaltninger bedst muligt introduceres?

SDU

Figur lavet på baggrund af Cybersikkerhed – helt sikkert, 2024

IT-sikkerheds strategi

Formål

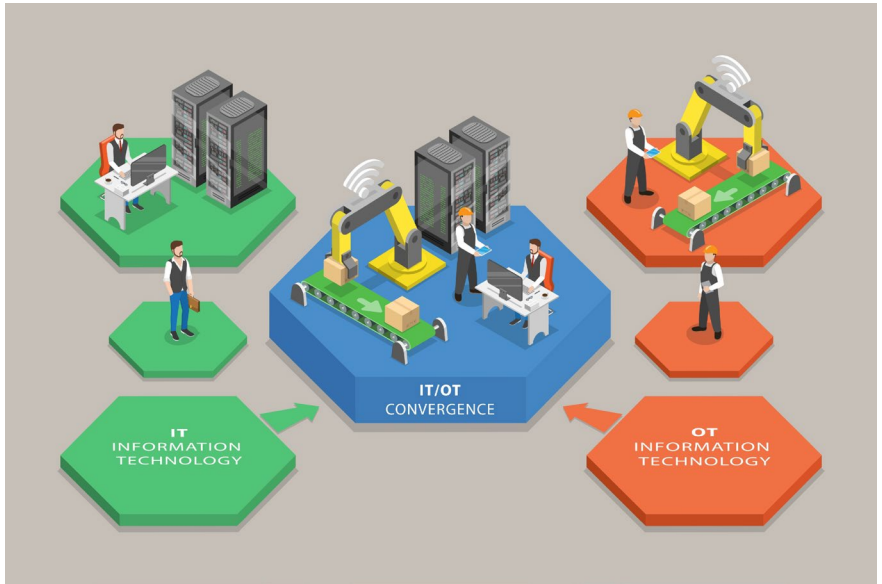
→Formålet med den nye strategi er at skabe et fremtidssikret og balanceret sikkerhedsgrundlag, hvor brugerne er medskabere af sikkerhedskulturen, og hvor teknologiske tiltag prioriteres efter risiko, kritikalitet og universitetets strategiske målsætninger

Scope for strategien

→ Oplægget er at der fastlægges nogle målbilleder og at strategien beskriver vejen derhen.
→ Med målbilleder menes der klare beskrivelser af, hvor vi ønsker, sikkerheden bevæger sig hen med udgangspunkt i best practice, der dog også tager højde for universitetets virkelighed og vilkår
  → Hvordan ser moderne it-sikkerhed ud sv.t. servere, netværk, storage, devices, software, identitetsstyring, cloud osv.
  → Hvordan får vi det til at balancere med universitetets kerneopgaver, som vi skal understøtte.
  → Geopolitiske spændinger, tyngdeforskydning, forskning i forsvarsteknologi, ledelsens risikoappetit
→ Fysisk sikkerhed herunder CCTV (overvågningskamera) – i første omgang udenfor scope
→ Styring af OT/CTS er umiddelbart med i scope.

OT (operationel teknologi)

Begreb	Betydning	Eksempel
OT (Operational Technology)	Teknologier, der styrer og overvåger fysiske processer og maskiner	CTS, laboratorieudstyr, adgangskontrol, ventilation, robotter
CTS (Central Tilstandskontrol og Styring)	Et **specifikt OT-system** der styrer bygningstekniske installationer som varme, ventilation, køling og energi	CTS-anlæg i bygningerne på universitetet (eks. Siemens Desigo, Schneider EcoStruxure)



OBS

→ Mange anskaffelser er også software anskaffelser
- → Når vi køber en dør med elektronisk lås
- → Overvågningskamera
- → Varmepumpe
- → 3D-printer

Styrelsen for Samfundssikkerhed

SAMSIK opfordrer organisationer til at gennemgå sikkerheden for deres operationel teknologi (OT)

01.09.2025

På baggrund af cyberangreb rettet mod operationel teknologi opfordrer SAMSIK organisationer til at gennemgå sikkerheden i deres OT-systemer.

Styrelsen for Samfundssikkerhed (SAMSIK) opfordrer organisationer til at gennemgå sikkerheden for deres operationel teknologi (OT). Det skyldes, at der det seneste år har været en række cyberangreb rettet mod OT-systemer i Europa. I flere af disse tilfælde er det lykkedes hackere at kompromittere og manipulere OT-systemerne, ofte fordi de har været utilstrækkeligt beskyttede. Blandt andet OT i vandsektoren har været mål for angreb, herunder et dansk vandværk, som i december 2024 fik kompromitteret og manipuleret et OT-system. Andre sektorer har dog også været mål for lignende angreb.

Modellen beskriver 5 søjler og 3 tværgående funktioner

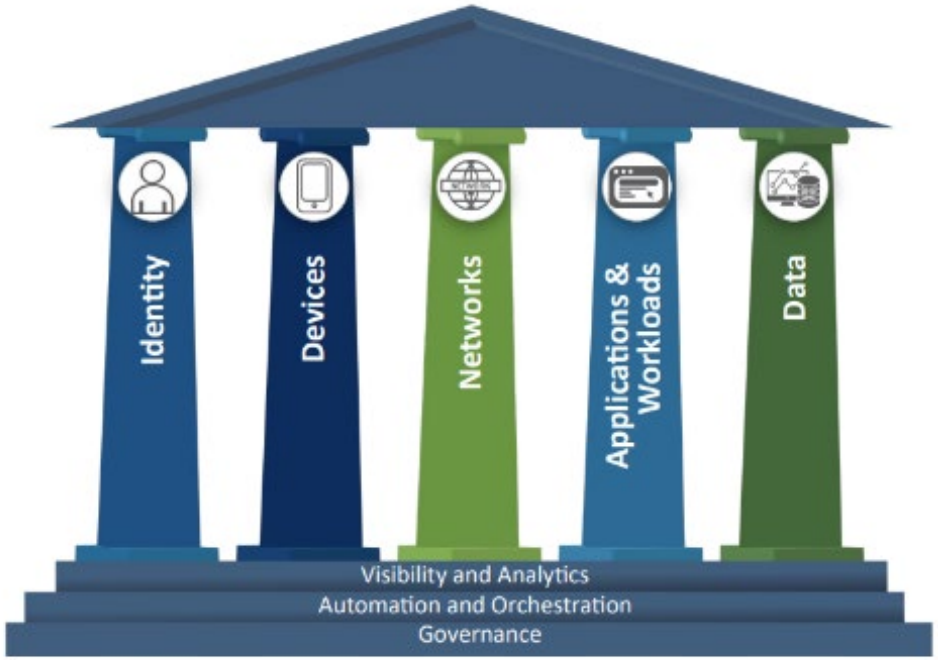


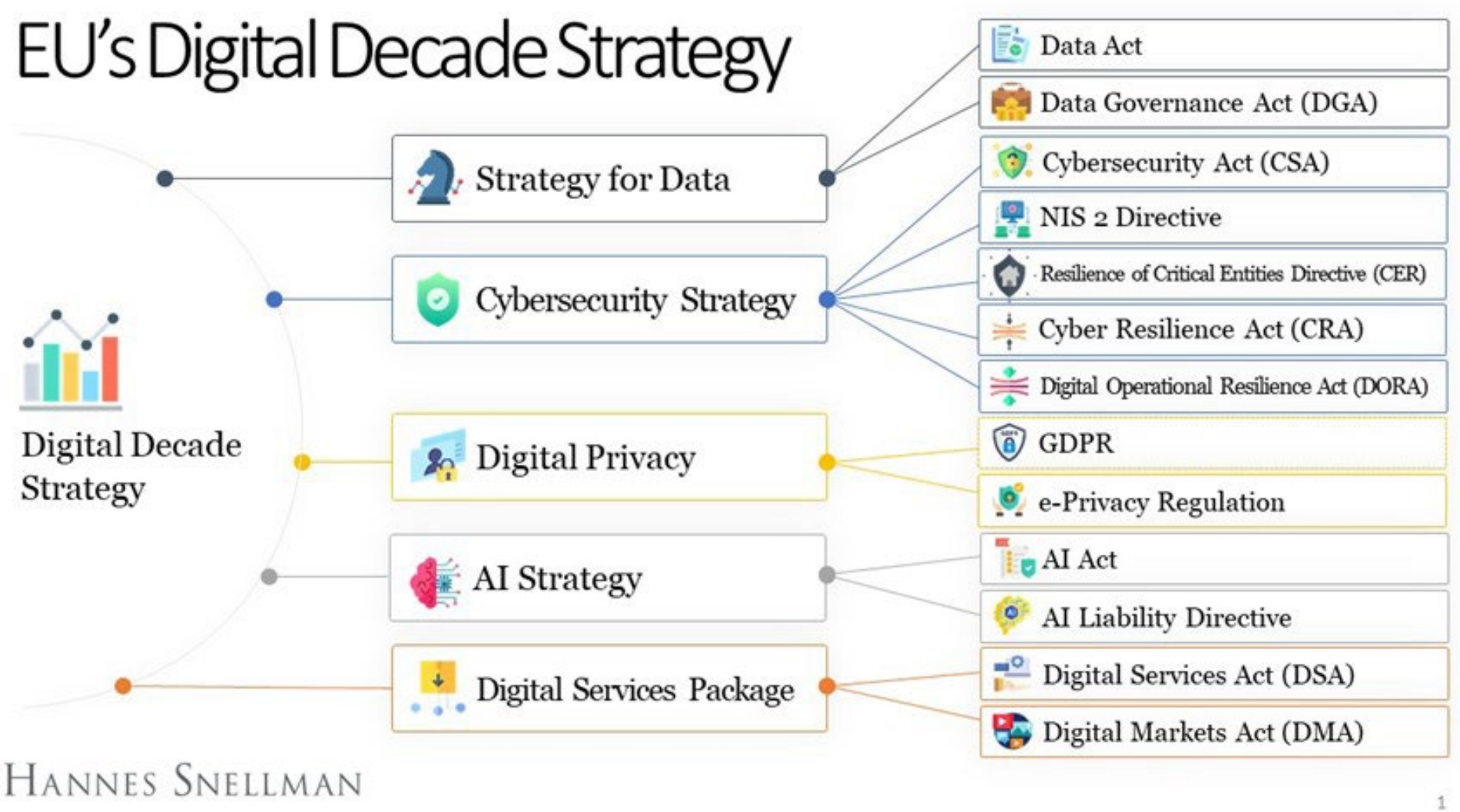
Figure 1: Zero Trust Maturity Model Pillars[5]

4 modenhedsniveauer for hver søjle og funktion

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

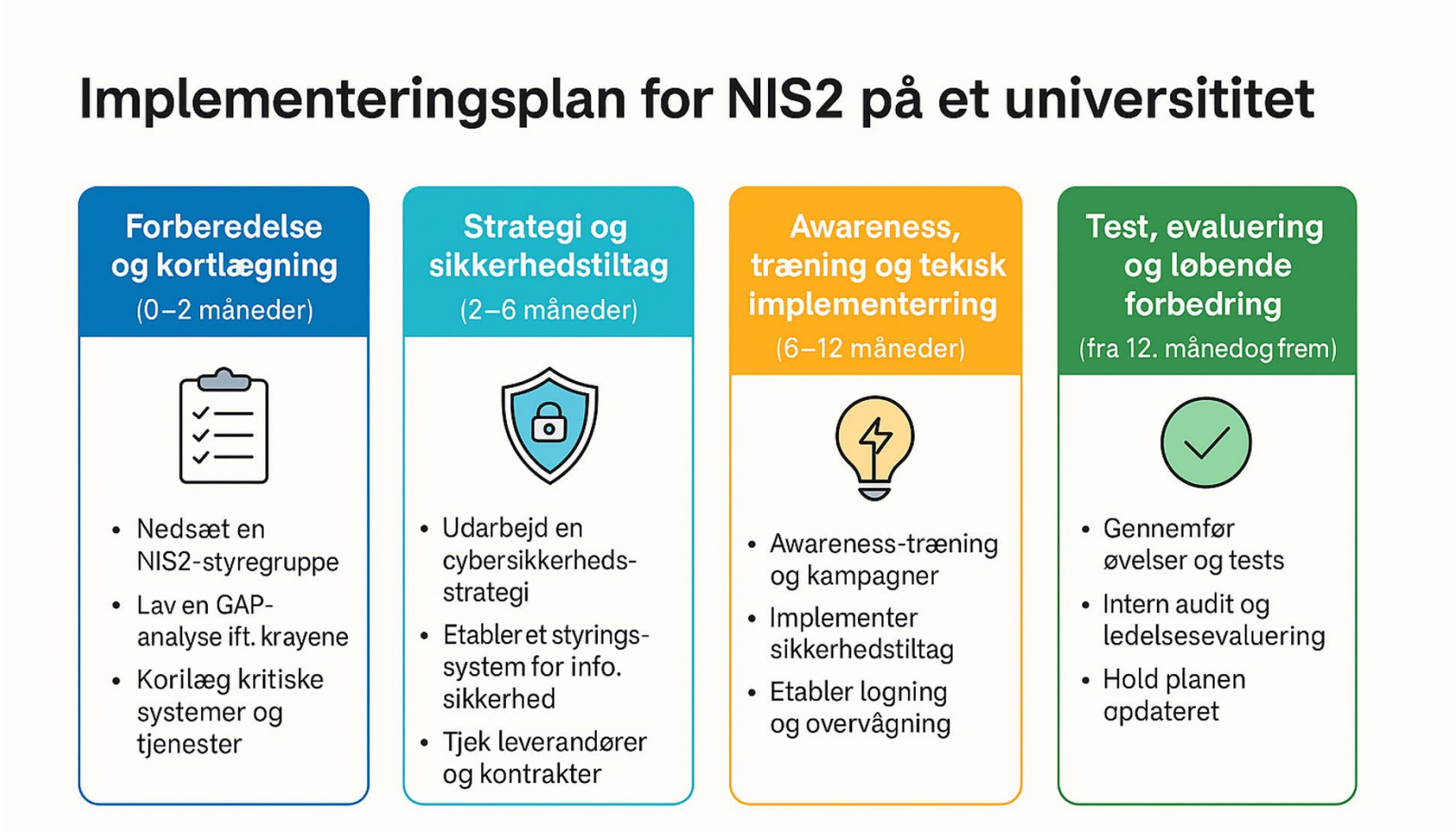
Figure 4: High-Level Zero Trust Maturity Model Overview

NIS2 implementering



https://www.hannessnellman.com/news-views/blog/the-hitchhiker-s-guide-to-the-digital-decade-prologue/

Vi kan spørge AI?



Konkrete hjælpeværktøjer

Vejledningsskema for cybersikkerhedsforanstaltninger

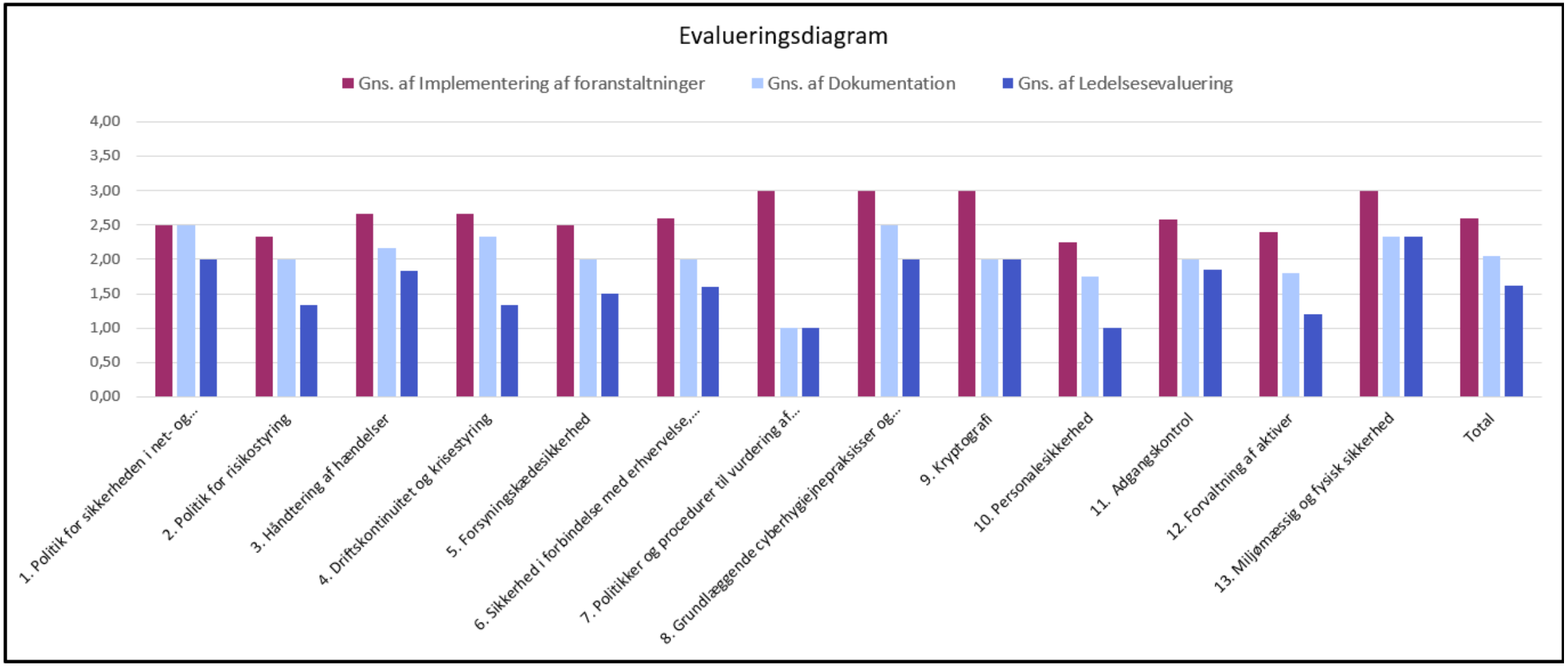
Foranstaltninger				Relaterede standarder				Selvevaluering (1-4)		
Henvising til gennemførselsforordning nr. 2024/2690's bilag	Kontrolmål	Kontroller	Gennemgangsbetingelser	ISO-standard	NIST-standard	ETSI-standard	CEN/TS-standard	Implementering af foranstaltninger	Dokumentation	Ledelsesevaluering jf. §7
1. Politik for sikkerheden i net- og informationssystemer										
1.1. Politik for sikkerheden i net- og informationssystemer	Relevante enheder etablerer og opretholder en sikkerhedspolitik for net- og informationssystemer, der fastlægger den overordnede tilgang til sikkerheden. (2022/2555, artikel 21, stk. 2, litra a).	Med henblik på artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 skal politikken for sikkerhed i net- og informationssystemer: (a) fastsætte de relevante enheders tilgang til styring af sikkerheden i deres net- og informationssystemer (b) være passende i forhold til og supplere de relevante enheders forretningsstrategi og -mål (c) fastsætte net- og informationssikkerhedsmål (d) omfatte en forpligtelse til løbende at forbedre sikkerheden i net- og informationssystemer (e) omfatte en forpligtelse til at stille de nødvendige ressourcer til rådighed til dens gennemførelse, herunder det nødvendige personale, de nødvendige finansielle ressourcer, samt de nødvendige processer, værktøjer og teknologier (f) meddeles til og anerkendes af relevante medarbejdere og relevante interesserede eksterne parter (g) fastsætte roller og ansvarsområder i henhold til Gennemførelsesforordningen pkt. 1.2 (h) omfatte en liste over den dokumentation, der skal opbevares, og en angivelse af, hvor længe denne dokumentation skal opbevares (i) omfatte en liste over emnespecifikke politikker (j) fastsætte indikatorer og foranstaltninger til overvågning af politikkens gennemførelse og den aktuelle status for modenheden af de relevante enheders net- og informationssikkerhed (k) omfatte en angivelse af datoen for ledelsesorganernes formelle godkendelse af de relevante enheder ("ledelsesorganerne") (2024/2690, pkt. 1.1.1.).	Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører politikken for sikkerheden i net- og informationssystemer mindst én gang om året, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici. Resultatet af hver gennemgang skal dokumenteres (2024/2690, pkt. 1.1.2.).	**ISO 27001:2022** 5.2, A.5.1, A.5.36, A.5.4, 9.3	**NIST CSF v2.0** PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, Clause 6.3	**CEN/TS 18026:2024** ISP-01, ISP-02, OPS-01, OPS-02, OPS-03	3	3	3
1.2. Roller, ansvarsområder og bemyndigelser	De relevante enheder fastlægger som led i deres sikkerhedspolitik for net- og informationssystemer, jf. Gennemførselsforordningen pkt. 1.1, ansvarsområder og bemyndigelser i forbindelse med sikkerheden i net- og informationssystemer, indordner dem pr. rolle, fordeler dem i overensstemmelse med de relevante enheders behov og meddeler dem til ledelsesorganerne (2024/2690, pkt. 1.2.1.).	De relevante enheder skal kræve, at alt personale og alle tredjeparter anvender et sikkerhedsniveau i deres net- og informationssystemer i overensstemmelse med de relevante enheders etablerede politik for net- og informationssikkerhed, emnespecifikke politikker og procedurer. Mindst én person skal rapportere direkte til ledelsesorganerne om spørgsmål vedrørende sikkerheden i net- og informationssystemer. Afhængigt af de relevante enheders størrelse skal sikkerheden i net- og informationssystemer være omfattet af særlige roller eller opgaver, der udføres, ud over de eksisterende roller. Modstridende forpligtelser og modstridende ansvarsområder adskilles, hvor det er relevant (2024/2690, pkt. 1.2.2., 1.2.3., 1.2.4. & 1.2.5.).	Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører rollerne, ansvarsområderne og bemyndigelserne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 1.2.6.).	**ISO 27001:2022** 5.3, A.5.2, A.5.3, A.5.4	**NIST CSF v2.0** GV.RR-02, GV.SC-02, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.1.2-01, REQ-7.2-01X, REQ-7.2-03X, REQ 7.2-07X, REQ 7.2-08X, REQ 7.2-09X, REQ 7.2-10X, REQ 7.2-11X,	**CEN/TS 18026:2024** ISP-02, OIS-02	3	3	3

https://digst.dk/tilsyn/nis-2/vejledningsmateriale-maalrettet-den-digitale-sektor/

Måler på en anden skala end klassisk ISO-modenhed

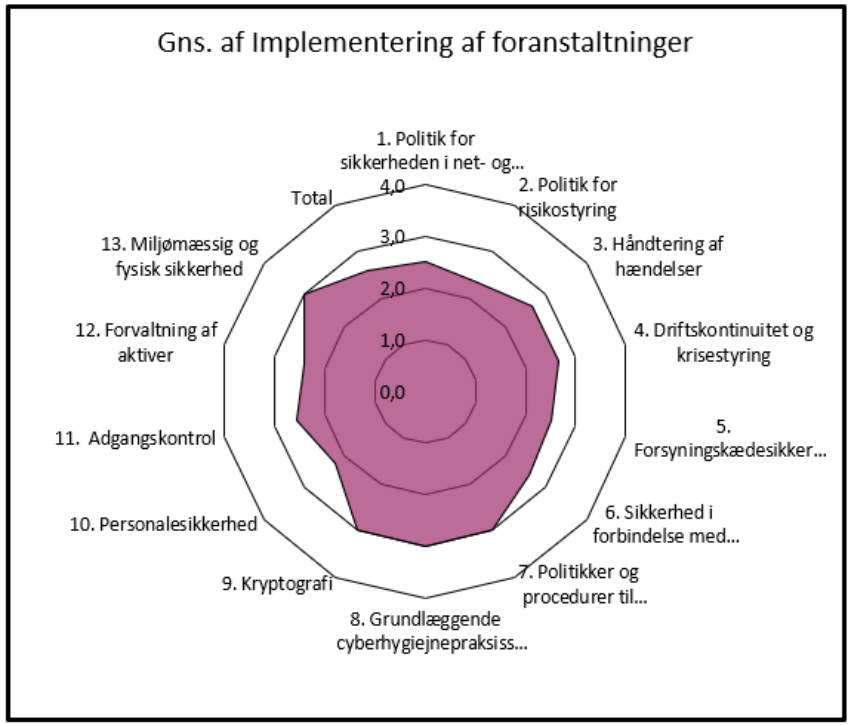
Selvevaluering: værdier og beskrivelse

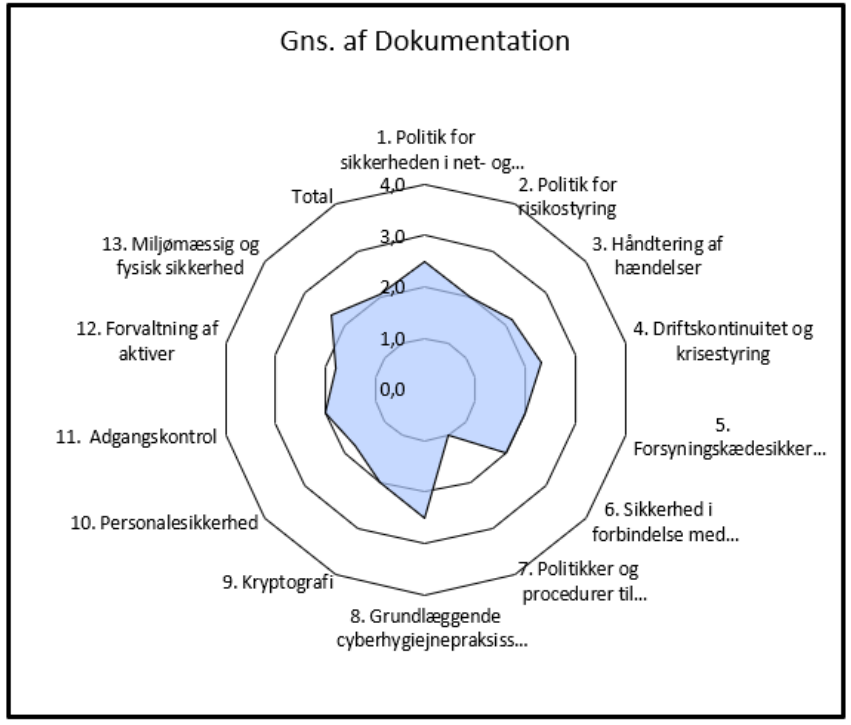
		Implementering af foranstaltninger	Dokumentation	Ledelsesevaluering jf. §7
Beskrivelse		Den pågældende kontrol/foranstaltning er implementeret i overensstemmelse med kravene i gennemførselsforordning 2024/2690.	Implementeringen af den pågældende foranstaltning er dokumenteret med henblik på, at dokumentationen i relevant omfang understøtter den løbende drift og videreudvikling, organisatorisk læring og ledelsens tilsyn.	Der er etableret procedure for at sikre, at ledelsen – som led i sit tilsyn – regelmæssigt forholder sig til og træffer beslutning om, hvorvidt den implementerede foranstaltning har den fornødne effekt.
Betydning af værdier	1	*Foranstaltningen er hverken implementeret eller planlagt*	*Dokumentation er hverken udarbejdet eller planlagt udarbejdet*	*En procedure er hverken etableret eller planlagt*
	2	*Foranstaltningen er planlagt, men ikke implementeret*	*Dokumentation er planlagt, men ikke udarbejdet*	*En procedure er planlagt, men ikke etableret*
	3	*Foranstaltningen er delvist implementeret*	*Dokumentation er delvist udarbejdet*	*En procedure er delvist implementeret*
	4	*Foranstaltningen er fuldt implementeret*	*Dokumentation er fuldt udarbejdet*	*En procedure er fuldt implementeret*
	Ikke relevant	*Det er ikke relevant at angive et svar i denne kategori*	*Det er ikke relevant at angive et svar i denne kategori*	*Det er ikke relevant at angive et svar i denne kategori*

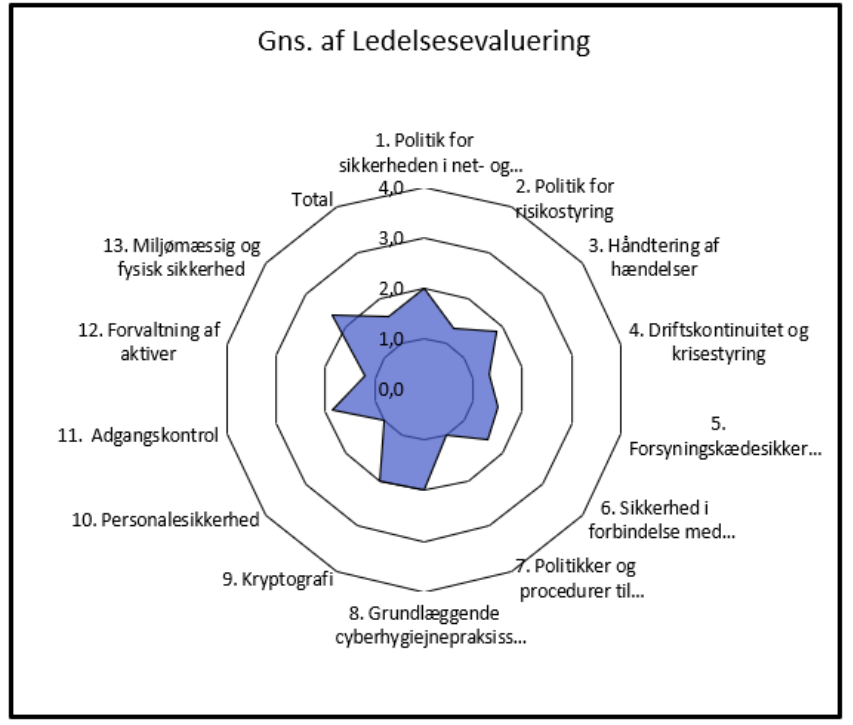


Fiktive modenhedstal – lavet til demonstration

Implementeringsgrad







Fiktive modenhedstal – lavet til demonstration

Key point – få styr på de grundlæggende forudsætninger

Forudsætning for at kunne implementere foranstaltninger

→ Placering af roller og ansvar (procesejer, systemejer, dataejer)

→ Risikostyring og afklaring af risikoappetit
  → Dataklassifikation (kritikalitet afgør ”passende” foranstaltninger)

SDU HR, Arbejdsmiljø og HR Udvikling

SDU medarbejderkurser

Kursusbeskrivelse | Har du spørgsmål? | Tilmelding

Risikovurderingsworkshop den 25. september 2025

Hvad er kurset formål?
At styrke deltagernes evne til at anvende risikovurderinger som et strategisk værktøj i praksis og sikre en ensartet tilgang på tværs af organisationen. Deltagerne arbejder med egne eller relevante cases og får faglig sparring fra GRC-teamet – herunder DPO, IT-konsulenter samt GDPR- og informationssikkerhedsspecialister.

Hvad er kurset målgruppe?
Workshoppen henvender sig til dig, der arbejder praktisk med risikovurderinger – fx som systemforvalter, IT-konsulent eller som GDPR- eller informationssikkerhedskoordinator med en rådgivende eller koordinerende rolle i risikovurderingsprocessen.

Hvad er kursets udbytte?
Workshoppen giver mulighed for:

- At gennemføre risikovurderinger med støtte fra erfarne rådgivere
- At få konkret feedback og kvalitetssikring af dit arbejde
- At sparre med andre deltagere og udveksle erfaringer og metoder

Workshoppen understøtter en fælles og systematisk tilgang til risikovurdering og giver deltagerne mulighed for at udveksle erfaringer og metoder med andre i organisationen. Der arbejdes med konkrete risikovurderinger, og deltagerne får feedback og støtte til at kvalificere deres arbejde.

Undervisere
Workshoppen afholdes som fysisk møde og faciliteres af GRC-teamet.

Systemforvaltningsaftale

Systemforvaltningsaftalen tager udgangspunkt i Økonomistyrelsens model for porteføljestyring af statslige IT-systemer. Modellen består af seks kortlægningsdimensioner:

© Økonomistyrelsen

Spørgsmål?