GLOBETEAM

NIS2 operationalisering

Ved Morten Eeg
Ejrnæs Nielsen

GLOBETEAM

Loven

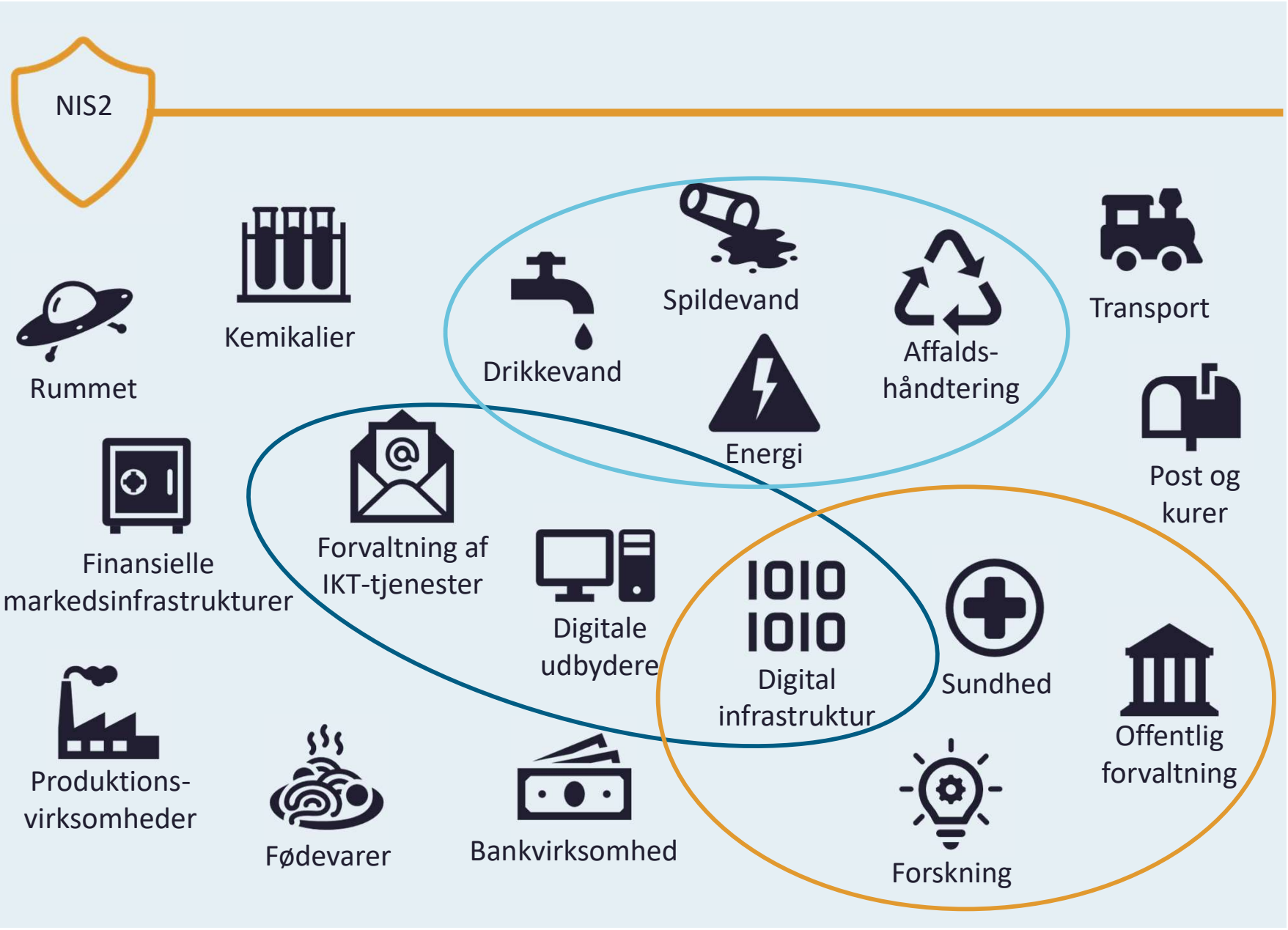
- Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Fokus

Tilgængelighed af tjenester, der er vigtige for samfundet!


NIS2
Rummet
Sundhed
Drikkevand
Spildevand
Digital infrastruktur
Post og kurer
Bankvirksomhed
Digitale udbydere
Forvaltning af IKT-tjenester
Finansielle markedsinfrastrukturer
Energi
Transport
Offentlig forvaltning
Produktions-virksomheder
Fødevarer
Affalds-håndtering
Forskning
Kemikalier

GLOBETEAM


NIS2
Rummet
Kemikalier
Drikkevand
Spildevand
Affalds-
håndtering
Transport
Energi
Post og
kurer
Finansielle
markedsinfrastrukturer
Forvaltning af
IKT-tjenester
Digitale
udbydere
Digital
infrastruktur
Sundhed
Offentlig
forvaltning
Produktions-
virksomheder
Fødevarer
Bankvirksomhed
Forskning

GLOBETEAM

Direkte eller indirekte omfattet

- Organisationer der er direkte omfattet, falder ind under alle direktivets krav og sanktioner.
- Organisationer der er indirekte omfattet, vil skulle leve op til de kontraktlige krav, som deres kunder/samarbejdspartnere stiller til dem, men vil ikke selv kunne sanktioneres som følge af direktivet.
- Det betyder både krav om ledelsens involvering, krav om sikkerhedstiltag, og krav om understøttelse i forhold til rapportering.

Krav til leverandører og samarbejdspartnere

Da direktivet har fokus på tilgængeligheden af omfattede tjenester, indeholder det også krav om sikkerhed hos leverandører og samarbejdspartnere.

Jo mere kritisk en leverandør eller samarbejdspartner er, jo større krav vil det være nødvendigt at stille, ud fra en risikobaseret tilgang.

§3

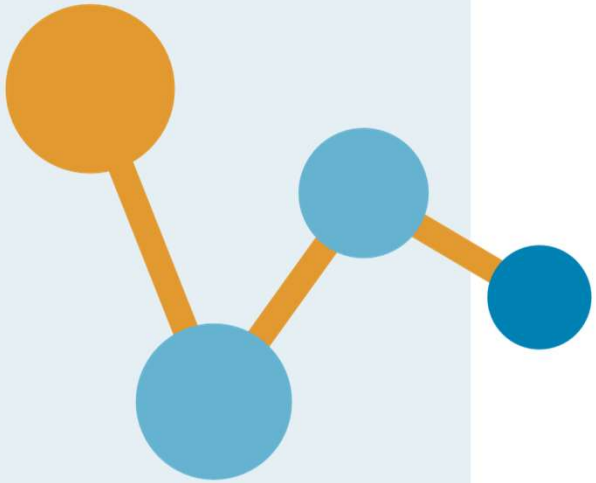
GLOBETEAM

Net- og Informationssystemer

a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder net-elementer, der ikke er aktive, som gør det muligt at overføre signaler.

b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.

c) Digitale data som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.



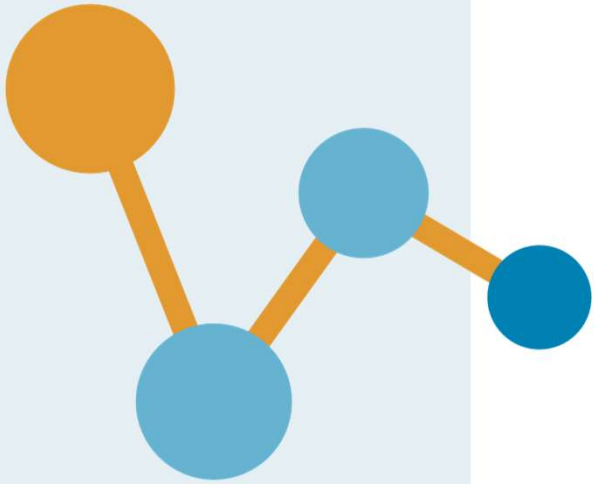
”oversættelse”

a) Alle systemer

b) Alt hardware

c) Alle data

d) Alle leverandører



Som er relevante for, at virksomheden kan levere sin omfattede tjeneste

Krav fra loven

Loven sætter krav inden for tre forskellige områder.

1. Ledelsesforankring (§7)
2. Foranstaltninger til styring af cybersikkerhedsrisici (§6)
3. Underretninger (§12)

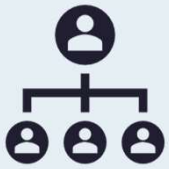
§3

Risikobaseret tilgang

Omfattede 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
- for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

GLOBETEAM



Informationssikkerhed

Udgangspunkt i organisationen

GDPR

Udgangspunkt i datasubjekterne

NIS2

Udgangspunkt i samfundet

Udgangspunkt i samfundet

Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til:

- graden af enhedens eksponering for risici,
- enhedens størrelse
- sandsynligheden for hændelser og deres alvor
- deres **samfundsmæssige** og økonomiske indvirkning.

NIS2 timeline

NIS2 for virksmheder

2023

Virksomheder reagerer

Virksomhederne forsøger at forstå de nye krav

NIS2 implementering

Valg af rammeværk

Hvor skal man starte?

Der er behov for rådgivning og rammeværk

- **ISO27001** – Governance på informationssikkerhed
- **NIST-CSF** – Governance på informationssikkerhed
- **D-mærket** – Governance men overfladisk, og på flere områder
- **CIS18** – Tekniske kontroller
- **Sikkerdigital** – Tekniske krav

Certificering eller mærkning er IKKE lig compliance

Hvor skal man starte?

Min klare anbefaling:

- **ISO27001** – rammeværk til styring af informationssikkerhed
- **ISAE3000 (NIS2)** – Dokumentation af kontroller
- Det er den måde revisorer vil dokumentere jeres overholdelse med direktivets krav.

ISAE3000

GLOBETEAM

Kontrolmål 4 – Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem virksomheden og dens direkte leverandører eller tjenesteudbydere. **Der foreligger formaliserede procedurer og kontroller for at sikre, at relevante og direkte tjenesteudbydere (herunder underleverandører) igennem hele leverandørkæden identificeres og overvåges for at sikre overholdelse af virksomhedens sikkerhedskrav og serviceleveranceaftaler.**			
Nr.	NIS2-*Serviceleverandørens kontrolaktivitet*	*Revisors udførte vurdering*	*Resultat af revisors vurdering*
4.4	Virksomheden overvåger løbende væsentlige leverandører for at sikre overholdelse af sikkerhedsforanstaltninger, håndtering af hændelser, væsentlige ændringer mv.	Forespurgt, om processen for identifikation og overvågning af væsentlige underleverandører. Inspiceret, ved en stikprøve på XX, at virksomheden har udført overvågning af væsentlige underleverandører for at sikre efterlevelse af sikkerhedskrav.	
4.5	Der foreligger procedurebeskrivelser for at sikre, at NIS2-relaterede serviceleverandører, som virksomheden anvender, identificeres.	Inspiceret, at en formaliseret procedure er designet og implementeret for at sikre NIS2 relevante leverandører bliver identificeret. Inspiceret, at proceduren er ledelses godkendt årligt eller ved ændringer i processen. Inspiceret, listen over NIS2 relevante leverandører.	
4.6	Alle identificerede kritiske NIS2-relaterede leverandører og tjenester undergår periodisk og som minimum en årlig risikovurdering af både tekniske og ikke-tekniske faktorer.	Forespurgt, om processen for periodisk risikovurdering af NIS2 relevante leverandører. Inspiceret, ved en stikprøve på XX, at virksomheden har foretaget risikovurdering af NIS2 relevante leverandører for både teknisk og ikke-tekniske faktorer.	
4.7	Kontrakter med vitale NIS2-relaterede udbydere indeholder passende sikkerhedskrav, der er baseret på risici, som er identificeret i forbindelse med risikovurderingen af serviceleverandøren.	Forespurgt, om processen for risikovurdering af NIS2 relevante leverandører. Inspiceret, at det anvendte rammeværk for risikovurdering, indeholder krav om vurdering mod relevante sikkerhedskrav. Inspiceret, ved en stikprøve på XX, at sikkerhedskrav afledt af risikovurderingen er indarbejdet i kontrakten med NIS2 relevante leverandører.	

GLOBETEAM

ISO27001 mapping

	ISO27002-2022	Controls	NIS2 Directive
5.	27002	**Organizational**	
5.1	27002	Policies for information security	20.1, 21.2(f)
5.2	27002	Information security roles and responsibilities	20.1, 21.2(b-c)
5.3	27002	Segregation of duties	21.2(i-j)
5.4	27002	Management responsibilities	20.1
5.5	27002	Contact with authorities	20.1, 21.2(b-c)+.3
5.6	27002	Contact with special interest groups	20.1, 21.2(b-c)+.3
5.7	27002	Threat intelligence	21.2(e+i-j)
5.8	27002	Information security in project management	21.1-.2(e+i)
5.9	27002	Inventory of information and other associated assets	21.1-.2(a+e+h-j)
5.10	27002	Acceptable use of information and other associated assets	20.1-.2, 21.1-.2(a+d-i)
5.11	27002	Return of assets	N/A
5.12	27002	Classification of information	21.1-.2(a+e+h-j)
5.13	27002	Labelling of information	21.1-.2(a+e+h-j)
5.14	27002	Information transfer	21.1-.2(a+e+h-j)
5.15	27002	Access control	21.2(i-j)
5.16	27002	Identity management	21.2(i-j)
5.17	27002	Authentication information	21.2(i-j)
5.18	27002	Access rights	21.2(i-j)
5.19	27002	Information security in supplier relationships	20.1, 21.2(d)+.3

Den tekniske tilgang

For at få overblik over de tekniske krav.

- **CIS18 og IEC62443** – Tekniske krav til IT og OT
- **Udfordringen** – Mangler det operationelle og organisatoriske fra direktivet

Derfor gerne kombineret med ISO27001 for den organisatoriske del, og stadig:

- **ISAE3000 (NIS2)** – Dokumentation af kontroller
- For at kunne dokumentere, at I lever op til kravene fra NIS2.

GLOBETEAM

CIS mapping

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Relationship	ISO Control #
2				Inventory and Control of Software Assets *Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*						
2	2,1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	X	X	X	Subset	5,9
2	2,4	Applications	Detect	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and		X	X		
2	2,5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		X	X	Subset	8.7
2	2,5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		X	X	Subset	8.19

Rammeværk hjælper

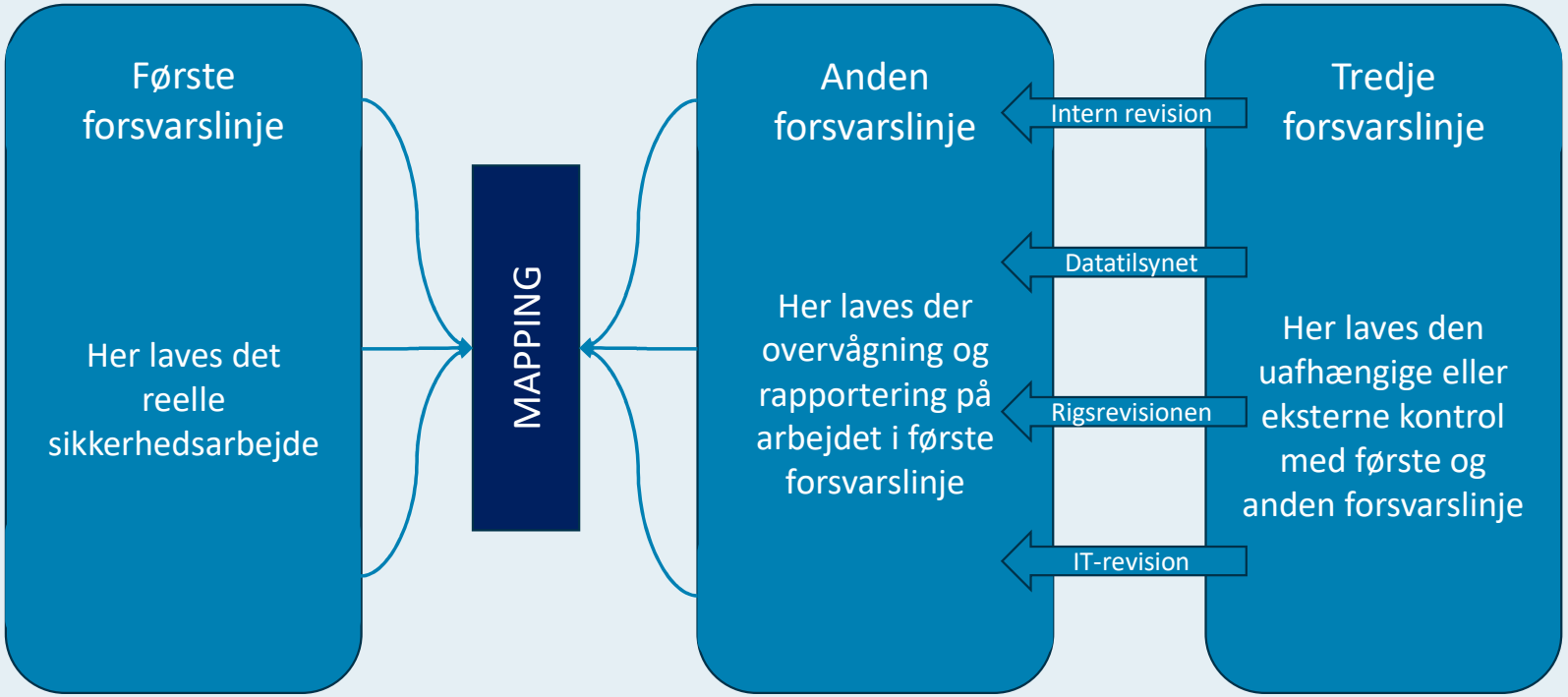
I metoden ”tre forsvarslinjer” samles alt sikkerhedsarbejdet på tværs af områder og krav i **første forsvarslinje**.

I **anden forsvarslinje** bliver arbejdet i den første linje overvåget og rapporteret til ledelsen.

I den **tredje forsvarslinje** er den uafhængige kontrol af arbejdet med sikkerhed.

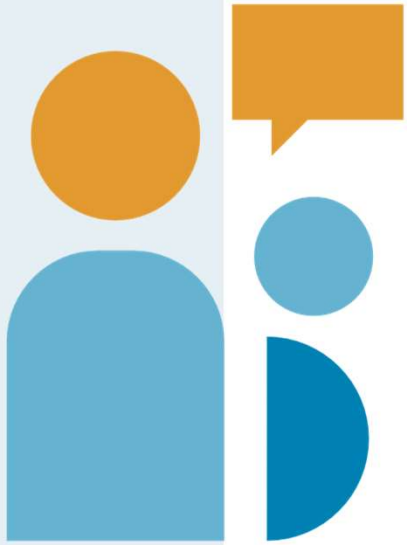
Uden rammeværk

Med rammeværk

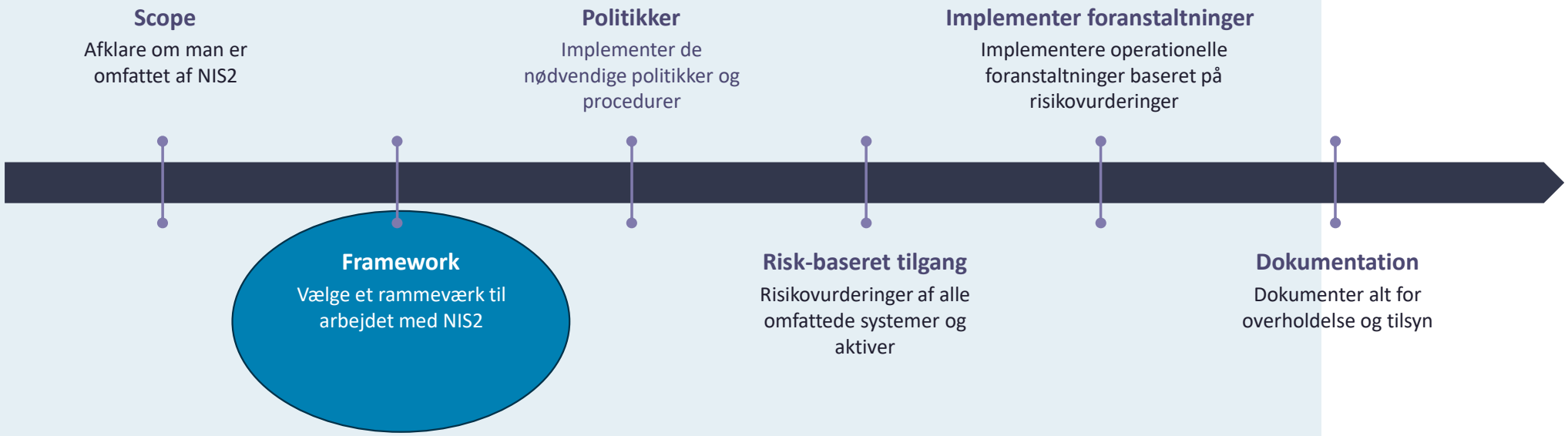


Mapping af krav

Foranstaltning	ISO27001	NIS2	CIS	IEC62443
Beredskab				
Risikovurdering				
To-faktor				
Segmentering				
Firewall				
Sårbarhedsscanning				



NIS2 timeline



NIS2 operationalisering

Hvor skal man starte?

Ved at vælge et rammeværk får man hjælp til **at definere, hvordan kravene fra NIS2 kan operationaliseres**. Men selv når man har valgt et rammeværk, betyder det ikke, at alle kontroller er nødvendige.

Arbejd med kontrollerne i rammen som med SoA-dokument. **Vælg dem, der er relevante**, og angiv årsagerne til, at resten er udeladt.

De følgende slides er eksempler på kontroller, valgt ud fra forskellige rammer og min egen erfaring.

De formelle krav

Direktivets krav (artikel 21 stk. 2 litra b):

b) Håndtering af hændelser

Lovens krav (§6 stk. 1 punkt 2):

2. Håndtering af hændelser

Kontrolmål

- Procedurer og kontroller er på plads for at sikre rettidig og korrekt håndtering af hændelser, herunder opdagelse, løsning og rapportering af hændelser til kunder.

Operationalisering af §6 stk. 1 punkt 2

Erfaringer fra projekter

- Etablering af en central overvågning af hele organisationens netværk.
- Retningslinjer for ensartet og standardiseret overvågning
- Fastlægge hvilken type hændelser, der vurderes som kritiske
- Procedurer der sikrer, at hændelser fra overvågningssystemer undersøges, deres indvirkning og konsekvens analyseres og forstås
- Standardiserede retningslinjer til rapportering om hændelsen
- Fastsættelse af kriterier for hvornår orientering af leverandører og aftagere af tjenesten om hændelsen, er nødvendig
- Kommunikationsstrategi til orientering af leverandører og aftagere af tjenesten

Operationalisering af §6 stk. 1 punkt 2

ISO27001

- Organisationen bør planlægge og forberede sig på at håndtere informationssikkerhedsincidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedsincidents (5.24)
- Organisationen bør vurdere informationssikkerhedshændelser og beslutte, om de skal kategoriseres som informationssikkerhedsincidents (5.25)
- Informationssikkerhedsincidents bør håndteres i overensstemmelse med de dokumenterede procedurer. (5.26)
- Organisationen bør planlægge og forberede sig på at håndtere informationssikkerhedsincidents ved at definere, etablere og kommunikere processer, roller og ansvar for styring af informationssikkerhedsincidents (5.27)

Operationalisering af §6 stk. 1 punkt 2

ISAE3000 (NIS2)

- Ledelsens ansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planlagt håndtering af informationssikkerhedshændelser vedrørende NIS2-tjenester
- Der er udarbejdet en plan og rammeværk for håndtering af større sikkerhedshændelser, som skal løses inden for en bestemt tidsramme.
- Der foreligger en ledelses overvågningskontrol for at sikre, at hændelser løses inden for en forud defineret tidsramme og i overensstemmelse med ledelsens forventninger.
- Procedurer og kontroller omfatter krav til rettidig identificering og registrering af væsentlige sikkerhedshændelser vedrørende relevante NIS2-underleverandører.
- Virksomheden udfører løbende test af hændelsesrapporteringsprocessen og mindst én gang årligt.

Operationalisering af §6 stk. 1 punkt 2

EU Kommissionens gennemførselsretsakt

- Hændelseshåndteringspolitik – herunder et kategoriseringssystem for hændelser, en kommunikationsplan, tildeling af roller og grænseflader mellem hændelseshåndteringen og forretningskontinuitetsstyring.
- Overvågning og logning – herunder procedurer og brug af værktøjer til at overvåge og logge aktiviteter på deres netværk, procedurer til at gennemgå logfiler, lister over overvågede aktiver og definere, hvordan man vedligeholder og sikkerhedskopierer logfiler i en foruddefineret periode og skal gemme logfilerne på et centralt sted og beskytte dem mod uautoriseret adgang.
- Hændelsesrapportering – inklusive en simpel mekanisme, der tillader deres medarbejdere, leverandører og kunder at rapportere mistænkelige hændelser.
- Hændelsesvurdering og klassificering – herunder vurder mistænkelige hændelser for at afgøre, om de udgør hændelser, og i givet fald bestemme deres art og alvor.
- Procedurer for reaktion på hændelser og reaktion efter hændelse – herunder indeslutning, udryddelse, genopretning, kommunikationsplaner for CSIRT og interessenter og logfiler og test af alle procedurer.

Operationalisering af §6 stk. 1 punkt 2

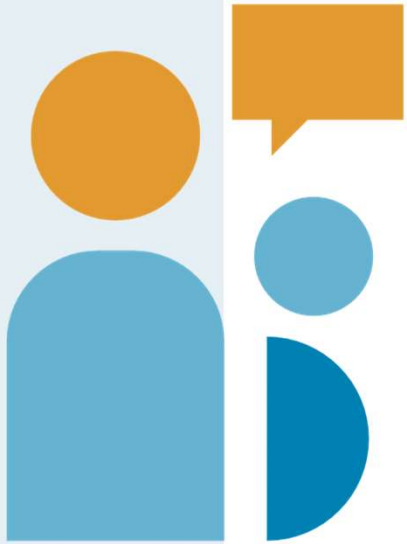
BCC framework

- Organisationen skal implementere en hændelsesproces, herunder roller, ansvar og myndigheder, og den skal udføres under eller efter en informations-/cybersikkerhedshændelse på organisationens kritiske systemer.
- Organisationen skal implementere et system (IDS) til at opdage cybersikkerhedshændelser.
- Organisationen skal undersøge oplysninger/cybersikkerhedsrelaterede meddelelser genereret fra systemerne (IDS).
- Organisationen skal implementere sårbarhedshåndteringsprocesser og -procedurer, der omfatter behandling, analyse og afhjælpning af sårbarheder fra interne og eksterne kilder.
- Organisationen skal implementere en hændelseshåndteringskapacitet for informations-/cybersikkerhedshændelser på sine forretningskritiske systemer, som omfatter forberedelse, detektion og analyse, indeslutning, udryddelse, genopretning og dokumenteret risikoaccept.

Hvad så?

Der er ikke nogen endegyldig rigtig eller korrekt måde at implementere NIS2!

- ❑ *Kig de forskellige rammeværk og metoder igennem og find ud af, hvad der passer bedst til jer.*
- ❑ *Beskriv hvorfor det passer bedst til jer, og jere valg/fravalg.*
- ❑ *Dokumenter alt hvad I gør.*



NIS2 kurser

Kursus om NIS2

NIS2 lead implementer certificering

Tak for jeres tid

Morten Eeg Ejrnæs Nielsen
men@globeteam.com
29 72 46 10

Scan QR-koden for nyheder om NIS2