Guide til Vejledningsskema for cybersikkerhedsforanstaltninger

1 Formål og brug

Vejledningsskemaet er udarbejdet i forbindelse med Digitaliseringsstyrelsens tilsynsførelse med enheder indenfor den digitale sektor, der er omfattet af NIS 2-loven. Hensigten med skemaet er at understøtte enhederne i deres arbejde med at forstå og implementere de konkrete krav til cybersikkerhedsforanstaltninger, som følger af NIS 2-reguleringen.

Skemaet kan overordnet bruges som:

- Vejledningsmateriale i forbindelse med den løbende implementering af cybersikkerhedsforanstaltninger,
- Redskab til at skabe overblik over compliance-krav for de enkelte områder.

Konkret kan enheden bruge skemaet som en del af sin interne proces til:

- at kortlægge nuværende status,
- at identificere eventuelle mangler,
- at rapportere status på enhedens implementering til enhedens ledelse.

---

2 Struktur og indhold

I dokumentet med vejledningsskemaet optræder fem faner:

Tabel 1 Overblik og beskrivelse af vejledningsskemaets fem faner.

Fane	Indhold
Introduktion	Den første fane introducerer skemaet og dokumentets indhold.
Vejledningsskema	Den anden fane består af selve vejledningsskemaet, som præsenterer et struktureret overblik over de krav, der stilles i gennemførselsforordning nr. 2024/2690's bilag, artikel 1-13. Her kan brugeren skabe overblik over foranstaltninger og udfylde selvevalueringsfelterne.
Selvevaluering_beskrivelse	Denne fane kan anvendes ved udfyldelse af vejledningsskemaets selvevalueringsfelter. Her beskrives felternes indhold, og hvordan man kan vurdere hvilken værdi, der skal angives.
Selvevaluering_output	I fjerde fane optræder data fra vejledningsskemaets selvevalueringsfelter, som visualiseres i diagrammer.
Diagramdata_låst	Denne fane er låst og skal ikke redigeres i af brugeren. Den optræder udelukkende af funktionelle årsager for dokumentet.

2.1 Vejledningsskema

Skemaet har til hensigt at give et struktureret overblik over de krav, der stilles i gennemførselsforordning nr. 2024/2690's **bilag, artikel 1-13**.

I skemaet er der for hver foranstaltning opstillet:

- hvilke kontrolmål og hvilke kontroller kravet omfatter,
- hvilke gennemgangsbetingelser, der gælder,
- hvilke internationale standarder (ISO, NIST, ETSI og CEN/TS), der relaterer til kravet.

Tabel 1 Overblik over vejledningsskemaets foranstaltninger.

Kontrolmål	Kontroller	Gennemgangsbetingelser	Standarder
Kontrolmål er de specifikke mål, en enhed skal opfylde for at sikre, at den overholder lovgivningens krav. Kontrolmålene fungerer som retningslinjer for, hvad der skal kontrolleres og opnås.	Kontroller er de konkrete handlinger eller procedurer, en enhed kan udføre for at sikre, at kontrolmålene opfyldes.	Gennemgangsbetingelser er de kriterier eller betingelser, der definerer, hvad der skal vurderes under en gennemgang af om en enhed efterlever lovens krav. Gennemgangsbetingelserne skal sikre, at kontrolmål og kontroller er opfyldt og udført korrekt.	Standarder er internationale eller nationale retningslinjer og specifikationer, der fastlægger krav og praksis indenfor cybersikkerhedsområdet. Standarderne anvendes til at sikre ensartethed og kvalitet i implementeringen af kontrolmål, kontroller og gennemgangsbetingelser.

Kolonnerne i vejledningsskemaet er opdelt på følgende måde:

Tabel 2 Overblik over vejledningsskemaets kolonner.

Kolonne	Emne	Forklaring
B	*Henvisning til forordningens artikel*	Angiver hhv. hvilken artikel og hvilket punkt i forordningen kravet udspringer fra
C, D	*Kontrolmål og kontroller*	Specificerer, hvad der forventes at være implementeret og hvordan
E	*Gennemgangsbetingelser*	Beskriver krav til hyppighed, ajourføring og dokumentation
F, G, H, I	*Relaterede standarder*	Viser hvilke anerkendte standarder, der understøtter efterlevelse
J, K, L	*Selvevalueringsfelter*	Her kan enheden selv dokumentere sin status for implementering, dokumentering og ledelsesevaluering.

2.2 Selvevaluering

Skemaet indeholder selvevalueringsfelter, der skal understøtte enhederne i deres vurdering af i hvor høj grad, de efterlever kravene i NIS 2-lovgivningen. Selvevalueringen er opdelt i tre kategorier: *Implementering af foranstaltninger* (om krav fra NIS 2 er implementeret), *Dokumentering* (om implementerede foranstaltninger er dokumenterede) og *Ledelsesevaluering jf. § 7* (om der er procedure for, at ledelsen løbende forholder sig til

foranstaltningen). For hver kategori er det muligt at angive sin selvevaluering på en skala fra 1-4. I skemaets anden fane, *Selvevaluering_beskrivelse*, findes beskrivelser af de tre kategorier. Her findes yderligere definitioner for besvarelsen samt en "Ikke relevant" kategori.

Besvarelserne er skaleret, så:

1. *= X er hverken planlagt eller implementeret/udarbejdet,*
2. *= X er planlagt, men ikke implementeret/udarbejdet,*
3. *= X er delvist implementeret/udarbejdet,*
4. *= X er fuldt implementeret/udarbejdet,*

hvor X afhænger af kategorien.

I fanen *Selvaevaluering_output* optræder de data, der er blevet indtastet i vejledningsskemaets selvevalueringsfelter i en overskuelig tabel. Vær opmærksom på, at pivottabellen skal opdateres efter, der er foretaget ændringer i Vejledningsskemaet. Data bliver desuden visualiseret i både et samlet søjlediagram samt et radardiagram for hver kategori.

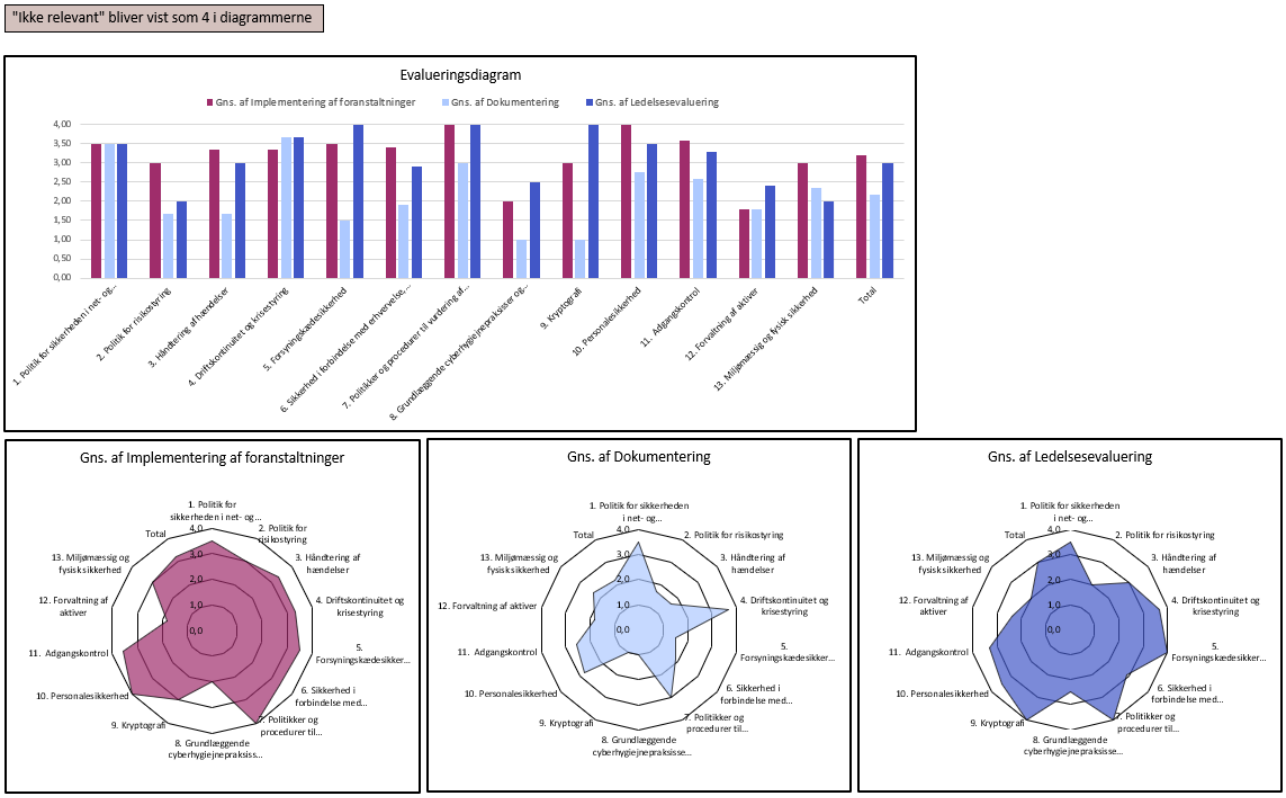
Figur 1 Eksempel på pivottabel baseret på output fra selvevalueringsfelterne i vejledningsskemaet.

HUSK: Opdater pivottabellen efter der er foretaget ændringer i Vejledningsskemaet (højreklik i pivotttabellen og vælg "Opdater").

Rækkemærkater	Gns. af Implementering af foranstaltninger	Gns. af Dokumentering	Gns. af Ledelsesevaluering
1. Politik for sikkerheden i net- og informationssystemer	**3,50**	**3,50**	**3,50**
1.1. Politik for sikkerheden i net- og informationssystemer	4,00	3,00	4,00
1.2. Roller, ansvarsområder og bemyndigelser	3,00	4,00	3,00
2. Politik for risikostyring	**3,00**	**1,67**	**2,00**
2.1. Ramme for risikostyring	3,00	2,00	2,00
2.2. Overvågning af overholdelse	2,00	1,00	3,00
2.3. Uafhængig gennemgang af informations- og netsikkerhed	4,00	2,00	1,00
3. Håndtering af hændelser	**3,33**	**1,67**	**3,00**
3.1. Politik for håndtering af hændelser	3,00	3,00	4,00
3.2. Overvågning og logning	4,00	1,00	2,00
3.3. Indberetning af begivenheder	4,00	1,00	4,00
3.4. Vurdering og klassifikation af begivenheder	2,00	2,00	2,00
3.5. Reaktion på hændelser	4,00	1,00	3,00
3.6. Gennemgang efter hændelsen	3,00	2,00	3,00
4. Driftskontinuitet og krisestyring	**3,33**	**3,67**	**3,67**
4.1. Driftskontinuitets- og katastrofeberedskabsplan	4,00	4,00	4,00
4.2. Styring af backups og reserver	3,00	4,00	3,00
4.3. Krisestyring	3,00	3,00	4,00
5. Forsyningskædesikkerhed	**3,50**	**1,50**	**4,00**
6. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- oginformationssystemer	**3,40**	**1,90**	**2,90**
7. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici	**4,00**	**3,00**	**4,00**
8. Grundlæggende cyberhygiejnepraksisser og sikkerhedsuddannelse	**2,00**	**1,00**	**2,50**
9. Kryptografi	**3,00**	**1,00**	**4,00**
10. Personalesikkerhed	**4,00**	**2,75**	**3,50**
11. Adgangskontrol	**3,57**	**2,57**	**3,29**
12. Forvaltning af aktiver	**1,80**	**1,80**	**2,40**
13. Miljømæssig og fysisk sikkerhed	**3,00**	**2,33**	**2,00**
Total	**3,20**	**2,16**	**3,00**

Eksempel på visualisering af output:

Figur 2 Eksempel på visualisering af output i form af søjle- og radardiagram.



3 Vigtigt at bemærke:

- Skemaet dækker de krav, der er direkte beskrevet i forordningens bilag.
- I de tilfælde, hvor der ikke forekommer tilstrækkelig information i forordningen, har DIGST tilføjet supplerende information. I de tilfælde er Digitaliseringsstyrelsen angivet som kilde.
- Henvisninger til internationale standarder er vejledende og kan anvendes som støtte til implementering.
- Kravene gælder hele enheden, medmindre andet fremgår af sektor- eller tjenestespecifik regulering.
- ENISA's tekniske guidelines, Technical Implementation Guidance, kan med fordel anvendes til at understøtte brugen af vejledningsskemaet.[1]
- Udfyldte selvevalueringer er kun for enheden selv, og oplysninger herfra vil ikke blive indsamlet eller gemt af DIGST.

[1] https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

4 Anvendt materiale

Udarbejdelsen af skemaet er sket på baggrund af direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet), lov nr. 434 af 6. maj 2025 om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) og EU's gennemførelsesforordning nr. 2024/2690. Gennemførselsforordningen specificerer NIS 2-direktivet og NIS 2-lovens krav, som enheder indenfor det digitale område skal efterleve. Derudover er ENISA's Technical Implementation Guidance vs. 1.0 anvendt i forbindelse med at sætte lovgivningens krav i relation til relevante standarder i vejledningsskemaet.