EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NATIONAL KAPACITETSVURDERING SRAMME

DECEMBER 2020

OM ENISA

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, har til formål at bidrage til målsætningen om et højt fælles niveau af cybersikkerhed i Europa. Den Europæiske Unions Agentur for Cybersikkerhed blev oprettet i 2004 og yderligere styrket ved EU's forordning om cybersikkerhed. Det bidrager til EU's politik for cybersikkerhed, fremmer troværdigheden af IKT-produkter, -tjenester og -processer gennem ordninger for cybersikkerhedscertificering, samarbejder med medlemsstater og EU-organer og ruster Europa til morgendagens cybersikkerhedsudfordringer. Gennem videndeling, kapacitetsopbygning og oplysningskampagner samarbejder agenturet med sine centrale interessenter om at styrke tilliden til den netforbundne økonomi, om at øge modstandsdygtigheden i EU's infrastruktur, og om i sidste instans at garantere EU's og EU-borgernes digitale sikkerhed. Yderligere oplysninger findes på www.enisa.europa.eu.

KONTAKT

Forfatterne kan kontaktes på team@enisa.europa.eu.
Ved pressehenvendelser vedrørende dette dokument benyttes press@enisa.europa.eu

FORFATTERE

Anna Sarri, Pinelopi Kyranoudi – Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

TAK

ENISA vil gerne takke og anerkende alle de eksperter, der deltog i og gav værdifulde input til denne rapport, navnlig følgende, i alfabetisk rækkefølge:

Afdelingen for cybersikkerhedspolitik, ministeriet for miljø, klima og kommunikation (Irland), James Caffrey

Center for Cybersikkerhed (Belgien)

CFCS – Center for Cybersikkerhed (Danmark), Thomas Wulff

Den italienske regering (Italien)

Den nationale sikkerhedsmyndighed (Slovakiet)

Den nationale sikkerhedstjeneste (Spanien), Maria Mar Lopez Gil

Det centrale statskontor for udvikling af det digitale samfund (Kroatien), Marin Ante Pivcevic

Det Europæiske Center for Bekæmpelse af Cyberkriminalitet – EC3, Alzofra Martinez Alvaro

Det Europæiske Center for Bekæmpelse af Cyberkriminalitet – EC3, Adrian-Ionut Bobeica

Det nationale cyber- og informationssikkerhedsagentur (Tjekkiet), Veronika Netolická

Forbundsministeriet for indre anliggender (Tyskland), Sascha-Alexander Lettgen

Informationssikkerhed i forvaltningen (Republikken Slovenien), Marjan Kavčič

Maltas agentur for informationsteknologi (Malta), Katia Bonello og Martin Camilleri

Ministeriet for digital politik (Grækenland), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali og Sotiris Vasilos

Ministeriet for retfærdighed og offentlig sikkerhed (Norge), Robin Bakke

Ministeriet for økonomi og kommunikation (Estland), Anna-Liisa Pärnalaas

NCTV, Justits- og sikkerhedsministeriet (Nederlandene)

Portugals nationale center for cybersikkerhed (Portugal), Alexandre Leite og Pedro Matos

University of Oxford – Center for global cybersikkerhedskapacitet, Carolin Weisser Harris

ENISA vil også gerne takke alle de eksperter, der har leveret input, men som foretrækker at forblive anonyme, for deres værdifulde bidrag til denne undersøgelse.

JURIDISK MEDDELELSE

Det skal bemærkes, at denne publikation repræsenterer ENISA's synspunkter og fortolkninger, medmindre andet er angivet. Denne publikation skal ikke fortolkes som en retlig foranstaltning truffet af ENISA eller et organ under ENISA, medmindre den vedtages i henhold til forordning (EU) nr. 2019/881.
Denne publikation repræsenterer ikke nødvendigvis den seneste udvikling, og ENISA kan til enhver tid opdatere publikationen.

Tredjepartskilder er citeret, hvor det er relevant. ENISA er ikke ansvarlig for indholdet af de eksterne kilder, herunder eksterne websteder, der henvises til i denne publikation.

Denne publikation offentliggøres alene til orientering. Den skal være tilgængelig gratis. Hverken ENISA eller nogen person, som handler på kontorets vegne, kan gøres ansvarlig for, hvordan oplysningerne i denne publikation anvendes.

MEDDELELSE OM OPHAVSRET

ISBN: 978-92-9204-476-3

DOI: 10.2824/02410

KATALOG: TP-02-21-253-DA-N

1. INDHOLDSFORTEGNELSE

ORDLISTE

AKRONYM	DEFINITION
AI	Kunstig intelligens
C2M2	Cybersecurity Capability Maturity Model
CCRA	Aftalen om anerkendelse af de fælles kriterier
CCSMM	Community Cybersecurity Maturity Model
CII	Kritisk informationsinfrastruktur
CMM	Cybersecurity Capacity Maturity Model for Nations
CMMC	Cybersecurity Maturity Model Certification
CPI	Cyber Power Index
CSIRT	Enheder, der håndterer IT-sikkerhedshændelser
CVD	Koordineret offentliggørelse af sårbarheder
DBM	Databeskyttelseslov
DSM	Digitalt indre marked
ECCG	Den Europæiske Cybersikkerhedscertificeringsgruppe
ECSM	Den europæiske måned for cybersikkerhed
ECSO	Den Europæiske Cybersikkerhedsorganisation
EFTA	Den Europæiske Frihandelssammenslutning
EQF	Europæisk referenceramme for kvalifikationer
EU	Den Europæiske Union
FoU	Forskning og udvikling
GCI	Globalt indeks for cybersikkerhed
GDPR	Generel forordning om databeskyttelse
GDS	Regeringens digitale tjeneste
IA-CM	Model til intern revisionsfunktion for den offentlige sektor
ICT	Informations- og kommunikationsteknologi
ISMM	Information Security Maturity Model til NIST's cybersikkerhedsramme
ITU	Den Internationale Telekommunikationsunion
LEA	Retshåndhævende agentur
MS	Medlemsstat

NCSS	Nationale strategier for cybersikkerhed
NIS	Net- og informationssikkerhed
NIST	National Institute of Standards and Technology
NLO	Nationale forbindelsesofficerer
OES	Operatører af væsentlige tjenester
OPP	Offentlig-private partnerskaber
OT	Driftsteknologi
PET	Teknologier til beskyttelse af privatlivet
PIMS	Informationsstyringssystem vedrørende databeskyttelse
Q-C2M2:	Qatar Cybersecurity Capability Maturity Model
SMV'er	Små og mellemstore virksomheder
SOG-IS MRA	Senior Officers Group for Information Systems' Security, aftale om gensidig anerkendelse

RESUMÉ

I takt med at det nuværende trusselsbillede vedrørende cybersikkerhed løbende udvides, og antallet af cyberangreb er stigende og mere omfattende, bliver EU's medlemsstater nødt til at gribe effektivt ind ved yderligere at udvikle og tilpasse deres nationale cybersikkerhedsstrategier (NCSS). Siden offentliggørelsen af ENISA's første NCSS-relaterede undersøgelser i 2012 har EU's medlemsstater og EFTA-landene gjort store fremskridt i forhold til at udvikle og gennemføre deres strategier.

I denne rapport beskrives ENISA's arbejde på at opbygge en national kapacitetsvurderingsramme (National Capabilities Assessment Framework, NCAF)

Formålet er at tilbyde medlemsstaterne en ramme for selvvurdering af deres modenhedsniveau ved at vurdere deres NCSS-mål, hvilket vil hjælpe dem med at styrke og opbygge kapacitet inden for cybersikkerhed, både på strategisk og operationelt plan.

Den giver et enkelt repræsentativt overblik over medlemsstaternes modenhed inden for cybersikkerhed. NCAF er et værktøj, der hjælper medlemsstaterne med at:

- Give nyttige oplysninger for udvikling af en langsigtet strategi (f.eks. god praksis, retningslinjer)
- Være med til at fastlægge de elementer, der mangler i NCSS'erne
- Bidrage til yderligere opbygning af cybersikkerhedskapaciteter
- Understøtte pålideligheden af politiske tiltag
- Styrke troværdigheden over for offentligheden og internationale partnere
- Støtte opsøgende arbejde og styrke dets omdømme i offentligheden som en gennemsigtig organisation
- Bidrage til at foregribe fremtidige problemstillinger
- Bidrage til at identificere indhøstede erfaringer og bedste praksis
- Definere en basislinje for cybersikkerhedskapaciteten i hele EU for at lette drøftelser
- Bidrage til at evaluere den nationale kapacitet inden for cybersikkerhed.

Denne ramme blev udformet med støtte fra ENISA's eksperter på området og repræsentanter fra 19 medlemsstater og EFTA-lande[1]. Rapportens målgruppe er politiske beslutningstagere, eksperter og embedsmænd, der er ansvarlige for eller er involveret i udformning, gennemførelse og evaluering af en NCSS og, mere generelt, cybersikkerhedskapacitet.

[1] Repræsentanter fra følgende medlemsstater og EFTA-lande blev interviewet: Belgien, Kroatien, Tjekkiet, Danmark, Estland, Tyskland, Grækenland, Ungarn, Irland, Italien, Liechtenstein, Malta, Nederlandene, Norge, Portugal, Slovakiet, Slovenien, Spanien, Sverige.

Den nationale kapacitetsvurderingsramme omfatter 17 strategiske mål og er opdelt i fire hovedgrupper:

- Gruppe nr. 1: Forvaltning af og standarder for cybersikkerhed
    1. Udvikle en national cyberberedskabsplan
    2. Definere grundlæggende sikkerhedsforanstaltninger
    3. Sikre digital identitet og opbygge tillid til digitale offentlige tjenester

- Gruppe nr. 2: Kapacitetsopbygning og bevidsthed
    4. Tilrettelægge cybersikkerhedsøvelser
    5. Etablere en beredskabsenhed
    6. Bevidstgøre brugere
    7. Styrke uddannelsesprogrammer
    8. Fremme FoU
    9. Give incitamenter til den private sektor til at investere i sikkerhedsforanstaltninger
    10. Forbedre cybersikkerheden i forsyningskæden

- Gruppe nr. 3: Love og administrative bestemmelser
    11. Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester
    12. Bekæmpe cyberkriminalitet
    13. Oprette mekanismer for indberetning af hændelser
    14. Styrke privatlivets fred og databeskyttelse

- Gruppe nr. 4: Samarbejde
    15. Etablere et offentligt-privat partnerskab
    16. Institutionalisere samarbejdet mellem offentlige organer
    17. Deltage i internationalt samarbejde

1. INDLEDNING

I henhold til direktivet om net- og informationssikkerhed (NIS), der blev offentliggjort i juli 2016, skal EU's medlemsstater vedtage en national strategi for sikkerheden i net- og informationssystemer, også kaldet en NCSS (national cybersikkerhedsstrategi), jf. artikel 1 og 7. En NCSS defineres i denne forbindelse som en ramme, der fastlægger strategiske principper, retningslinjer, strategiske mål, prioriteter og passende politiske og lovgivningsmæssige foranstaltninger. Det planlagte mål for en NCSS er at nå og opretholde et højt niveau af net- og systemsikkerhed og dermed gøre det muligt for medlemsstaterne at afværge potentielle trusler. Desuden kan NCSS også være en katalysator for industriel udvikling samt økonomisk og social fremgang.

I henhold til EU's forordning om cybersikkerhed skal ENISA fremme udbredelsen af bedste praksis i forbindelse med udformning og gennemførelse af en NCSS ved at støtte medlemsstaterne i tilpasningen af NIS-direktivet og ved at indsamle værdifuld feedback om deres erfaringer. Med henblik herpå har ENISA udviklet adskillige værktøjer til at bistå medlemsstaterne med at udvikle, gennemføre og evaluere deres nationale cybersikkerhedsstrategier (NCSS).

En af ENISA's opgaver er at udvikle en ramme for selvvurdering af national kapacitet for at måle modenheden af de enkelte NCSS'er. Formålet med denne rapport er at fremlægge den undersøgelse, der er gennemført i forbindelse med udformningen af rammen for selvvurdering.

1.1 UNDERSØGELSENS OMFANG OG FORMÅL

Hovedformålet med denne undersøgelse er at udarbejde en ramme for selvvurdering af national kapacitet, i det følgende benævnt NCAF, med henblik på at måle modenheden af medlemsstaternes cybersikkerhedskapacitet. Rammen bør konkret sætte medlemsstaterne i stand til at:

- Udføre vurderingen af deres nationale cybersikkerhedskapacitet
- Øge bevidstheden om landets modenhedsniveau
- Udpege områder, hvor der er plads til forbedringer
- Opbygge cybersikkerhedskapacitet.

Denne ramme bør hjælpe medlemsstaterne, og navnlig de nationale politiske beslutningstagere, med at foretage en selvvurdering med henblik på at forbedre den nationale cybersikkerhedskapacitet.

1.2 METODE

Den metode, der blev anvendt til at udvikle rammen for selvvurdering af national kapacitet, omfatter fire hovedfaser:

1. **Dokumentationsundersøgelse**: Den første fase bestod af en omfattende litteraturgennemgang for at indsamle bedste praksis vedrørende udvikling af en ramme for vurdering af nationale cybersikkerhedsstrategiers modenhed. Dokumentationsundersøgelsen er koncentreret om en systematisk analyse af relevante dokumenter om kapacitetsopbygning inden for cybersikkerhed og fastlæggelse af en strategi, om medlemsstaternes NCSS'er og om en sammenligning af eksisterende modenhedsmodeller for cybersikkerhed. Der blev gennemført en benchmarkøvelse for eksisterende modenhedsmodeller med vedtagelse af en

analysemetode, der blev udviklet med henblik på denne undersøgelse. Analysemetoden bygger på Becker[2]-metoden til udvikling af modenhedsmodeller, som fastsætter en generel og konsolideret proceduremodel til udvikling af modenhedsmodeller og opstiller klare krav til udviklingen af dem. Analysemetoden blev yderligere tilpasset med henblik på at opfylde behovene i denne undersøgelse.

2. **Indsamling af eksperters og interessenters synspunkter**: På grundlag af de data, der blev indsamlet via dokumentationsundersøgelsen og de dermed forbundne foreløbige resultater af analysen, omfattede denne fase udpegning og indbydelse af de udpegede eksperter, der har erfaring med udvikling og gennemførelse af en NCSS eller modenhedsmodeller, med henblik på interview. ENISA kontaktede sin ekspertgruppe vedrørende nationale cybersikkerhedsstrategier og nationale forbindelsesofficerer for at finde frem til de relevante eksperter i den enkelte medlemsstat. Derudover blev nogle eksperter, der var involveret i udviklingen af modenhedsmodeller, interviewet. Der blev i alt gennemført 22 interview, hvoraf 19 blev gennemført med repræsentanter for cybersikkerhedsagenturer i forskellige medlemsstater (og EFTA-lande).
3. **Analyse af input fra statusrapporten:** De data, der blev indsamlet gennem dokumentationsundersøgelsen og interviewene, blev efterfølgende analyseret for at identificere bedste praksis for udformningen af en ramme for selvvurdering til måling af NCSS'ernes modenhed, forstå medlemsstaternes behov og fastslå, hvilke data der kan indsamles i de forskellige europæiske lande[3]. Denne analyse gjorde det muligt at trimme den foreløbige model, der blev udviklet i de foregående faser, og finjustere sættet af indikatorer i modellen, modenhedsniveauerne og dimensionerne.
4. **Færdiggørelse af modellen:** Derefter blev en ajourført version af rammen for selvvurdering af national kapacitet gennemgået af ENISA's emneeksperter og efterfølgende godkendt af eksperter på en workshop, der blev afholdt i oktober 2020 forud for offentliggørelsen.

1.3 MÅLGRUPPE

Rapportens målgruppe er politiske beslutningstagere, eksperter og embedsmænd, der er ansvarlige for eller involveret i udformning, gennemførelse og evaluering af NCSS'en og mere generelt cybersikkerhedskapacitet. Desuden kan de resultater, der formaliseres i dette dokument, være nyttige for eksperter i cybersikkerhedspolitik og forskere på nationalt eller europæisk plan.

[2] J. Becker, R. Knackstedt og J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, s. 213–222, juni 2009.
[3] I denne undersøgelse omfatter de "europæiske lande", der henvises til i denne rapport, de 27 EU-medlemsstater.

2. BAGGRUND

2.1 TIDLIGERE ARBEJDE MED EN NCSS' LIVSCYKLUS

Som det fremgår af EU's lovgivning om cybersikkerhed, er et af ENISA's vigtigste mål at støtte medlemsstaterne i udviklingen af nationale strategier for sikkerhed i net- og informationssystemer, fremme udbredelsen af disse strategier og overvåge gennemførelsen af dem. ENISA har som led i sit mandat udarbejdet flere dokumenter om dette emne for at fremme udvekslingen af god praksis og støtte gennemførelsen af NCSS'er i hele EU:

- "Practical guide on the development and execution phase of NCSS"(praktisk vejledning om NCSS' udviklings og gennemførelsesfase [4], der blev offentliggjort i 2012
- "Setting the course for national efforts to strengthen security in cyberspace"[5], der blev offentliggjort i 2012
- Den første ENISA-ramme for evaluering af en medlemsstats NCSS, der blev offentliggjort[6] i 2014.
- "Online NCSS Interactive Map" (interaktivt kort til NCSS online)[7], der blev offentliggjort i 2014.
- "NCSS Good Practice Guide"[8], der blev offentliggjort i 2016.
- "National Cybersecurity Strategies Evaluation Tool" (evalueringsværktøj for nationale cybersikkerhedsstrategier)[9], der blev offentliggjort i 2018.
- "Good practices in innovation on Cybersecurity under the NCSS"[10], der blev offentliggjort i 2019.

BILAG A indeholder en kort oversigt over ENISA's vigtigste publikationer om dette emne.

Ovennævnte vejledninger og dokumenter blev gennemgået som led i dokumentationsundersøgelsen. Navnlig "National Cybersecurity Strategies Evaluation Tool" ([11] er et grundlæggende element i NCAF. NCAF bygger på de mål, der er beskrevet i NCSS-onlineevalueringsværktøjet.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] En evalueringsramme for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, ajourført i 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Dette dokument er en ajourføring af vejledningen fra 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 FÆLLES MÅL, DER ER FASTLAGT INDEN FOR RAMMERNE AF DEN EUROPÆISKE NCSS

Forskellene mellem de enkelte medlemsstater gør det vanskeligt at fastlægge fælles aktiviteter eller handlingsplaner på tværs af forskellige nationale sammenhænge, retlige rammer og politiske dagsordener. De strategiske mål for medlemsstaternes NCSS'er er imidlertid ofte formuleret omkring de samme emner. På grundlag af ENISA's tidligere arbejde og analysen af medlemsstaternes NCSS'er blev der således identificeret 22 strategiske mål. 15 af disse strategiske mål blev allerede identificeret i ENISA's tidligere arbejde, 2 blev føjet til under denne undersøgelse, og der blev udpeget 5 mål til efterfølgende behandling.

2.2.1 Fælles strategiske mål, der dækkes af medlemsstaterne

Baseret på ENISA's tidligere arbejde, nemlig National Cybersecurity Strategies Evaluation Tool[12], vises i nedenstående tabel ovennævnte 15 strategiske mål, der normalt indgår i medlemsstaternes NCSS'er. Målene beskriver kernen i den overordnede "nationale filosofi" om emnet. Yderligere oplysninger om de mål, der er beskrevet nedenfor, findes i ENISA's rapport om "NCSS Good Practice Guide"[13].

Tabel 1: Fælles strategiske mål, der dækkes af medlemsstaternes NCSS

ID	Strategiske mål i NCSS	Mål
1	**Udvikle nationale cyberberedskabsplaner**	▶ Fremlægge og forklare de kriterier, der bør anvendes til at definere en situation som en krise ▶ Fastlægge de vigtigste processer og tiltag til håndtering af krisen ▶ Klart definere de forskellige interessenters roller og ansvarsområder under en cyberkrise ▶ Fremlægge og gøre rede for kriterierne for, hvornår en krise er overstået, og/eller hvem der har beføjelse til at erklære dette.
2	**Definere grundlæggende sikkerhedsforanstaltninger**	▶ Harmonisere de forskellige praksisser, som organisationer i både den offentlige og den private sektor følger ▶ Skabe et fælles sprog mellem de kompetente offentlige myndigheder og organisationerne samt åbne sikre kommunikationskanaler ▶ Tillade forskellige interessenter at kontrollere og benchmarke deres cybersikkerhedskapacitet ▶ Udveksle oplysninger om god praksis inden for cybersikkerhed i alle erhvervssektorer ▶ Hjælpe interessenter med at prioritere deres investeringer i sikkerhed.
3	**Tilrettelægge cybersikkerhedsøvelser**	▶ Identificere, hvad der skal afprøves (planer og processer, mennesker, infrastruktur, indsatskapacitet, samarbejdskapacitet, kommunikation osv.) ▶ Oprette et nationalt team med et klart mandat til at planlægge cyberøvelser ▶ Integrere cyberøvelser i livscyklussen for den nationale cybersikkerhedsstrategi eller den nationale cyberberedskabsplan.
4	**Etablere en beredskabsenhed**	▶ Mandat – dette vedrører de beføjelser, roller og ansvarsområder, som den pågældende regering skal tildele teamet ▶ Tjenesteportefølje – dette omfatter de tjenester, som et team leverer til sine medlemmer eller anvender til sin egen interne funktion ▶ Operationel kapacitet – dette vedrører de tekniske og operationelle krav, som et team skal opfylde

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Dette dokument er en ajourføring af vejledningen fra 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strategiske mål i NCSS	Mål
		▶ Samarbejdskapacitet – dette omfatter krav til udveksling af oplysninger med andre teams, som ikke er omfattet af de foregående tre kategorier, f.eks. politiske beslutningstagere, militæret, lovgivere, operatører (kritisk informationsinfrastruktur) og retshåndhævende myndigheder.
5	Bevidstgøre brugere	▶ Identificere mangler i viden om spørgsmål vedrørende cybersikkerhed eller informationssikkerhed ▶ Afhjælpe manglerne ved at øge bevidstheden eller udvikle/styrke videngrundlaget.
6	Styrke uddannelsesprogrammer	▶ Forbedre de eksisterende informationssikkerhedsmedarbejderes operationelle kapacitet ▶ Tilskynde studerende til at beskæftige sig med og forberede dem på at beskæftige sig med cybersikkerhedsområdet ▶ Fremme og styrke forbindelserne mellem det akademiske miljø for informationssikkerhed og informationssikkerhedsindustrien ▶ Tilpasse uddannelse i cybersikkerhed til erhvervslivets behov.
7	Fremme af FoU	▶ Identificere de reelle årsager til sårbarheder i stedet for at udbedre virkningerne af dem ▶ Samle forskere fra forskellige fagområder for at finde løsninger på flerdimensionelle og komplekse problemer, såsom fysiske cybertrusler ▶ Samle industriens behov og forskningsresultater og dermed lette overgangen fra teori til praksis ▶ Finde måder til ikke kun at opretholde, men også øge cybersikkerhedsniveauet for produkter og tjenester, der understøtter eksisterende cyberinfrastrukturer.
8	Give incitamenter til den private sektor til at investere i sikkerhedsforanstaltninger	▶ Identificere mulige incitamenter for private virksomheder til at investere i sikkerhedsforanstaltninger ▶ Give virksomheder incitamenter til at fremme investeringer i sikkerhed.
9	Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester (CII)	▶ Identificere kritisk informationsinfrastruktur ▶ Identificere og afværge relevante risici for CII.
10	Bekæmpe cyberkriminalitet	▶ Udarbejde love vedrørende cyberkriminalitet ▶ Forbedre retshåndhævende myndigheders effektivitet.
11	Indføre mekanismer til indberetning af hændelser	▶ Opnå viden om det overordnede trusselsmiljø ▶ Vurdere konsekvenserne af hændelser (f.eks. brud på sikkerheden, netfejl, driftsafbrydelser) ▶ Indhente viden om eksisterende og nye sårbarheder og typer af angreb ▶ Ajourføre sikkerhedsforanstaltninger i overensstemmelse hermed ▶ Gennemføre NIS-direktivets bestemmelser om indberetning af hændelser.
12	Styrke privatlivets fred og databeskyttelse	▶ Bidrage til at styrke de grundlæggende rettigheder vedrørende privatlivets fred og databeskyttelse.
13	Etablere et offentligt-privat partnerskab (OPP'er)	▶ Afskrækkelse (for at afskrække angribere) ▶ Beskyttelse (anvender forskning i nye sikkerhedstrusler) ▶ Detektion (anvender informationsudveksling til at imødegå nye trusler) ▶ Reaktion (for at levere kapacitet til at håndtere de indledende konsekvenser af en hændelse) ▶ Genopretning (for at levere kapacitet til at udbedre den endelige konsekvens af en hændelse).
14	Institutionalisere samarbejdet mellem offentlige organer	▶ Øge samarbejdet mellem offentlige agenturer med ansvar for og kompetencer inden for cybersikkerhed ▶ Undgå overlapning af kompetencer og ressourcer mellem offentlige organer ▶ Forbedre og institutionalisere samarbejdet mellem offentlige agenturer på forskellige områder inden for cybersikkerhed.
15	Indgå i internationalt samarbejde (ikke kun med EU's medlemsstater)	▶ Drage fordel af at skabe en fælles videnbase mellem EU's medlemsstater

ID	Strategiske mål i NCSS	Mål
		▶ Skabe synergieffekter mellem nationale cybersikkerhedsmyndigheder ▶ Tillade og øge bekæmpelsen af grænseoverskridende kriminalitet.

2.2.2 Yderligere strategiske mål

På grundlag af ENISA's dokumentationsundersøgelse og de interview, der blev gennemført af ENISA, blev der fastlagt yderligere strategiske mål. Medlemsstaterne behandler i stigende grad disse emner i deres NCSS, eller de fastlægger handlingsplaner for samme emne. Der fremlægges også eksempler på aktiviteter, som medlemsstaterne har gennemført. Hvis et eksempel stammer fra en offentligt tilgængelig kilde, refereres der hertil. Når eksempler er baseret på fortrolige interview med EU-medlemsstaternes tjenestemænd, angives ingen referencer.

Der blev udpeget følgende yderligere strategiske mål:

- Forbedre cybersikkerheden i forsyningskæden og
- Sikre digital identitet og opbygning af tillid til digitale offentlige tjenester.

Forbedre cybersikkerheden i forsyningskæden

Små og mellemstore virksomheder (SMV'er) er rygraden i den europæiske økonomi. De udgør 99 % af alle virksomheder i EU[14], og i 2015 blev det anslået, at SMV'er har skabt omkring 85 % af de nye arbejdspladser og bidraget med to tredjedele af den samlede beskæftigelse i den private sektor i EU. Eftersom SMV'er desuden leverer tjenesteydelser til store virksomheder og i stigende omfang samarbejder med offentlige myndigheder[15], skal det bemærkes, at SMV'er i den nuværende indbyrdes forbundne kontekst udgør det svage led i tilfælde af cyberangreb. SMV'er er de mest udsatte for cyberangreb, men de har ofte ikke råd til at investere tilstrækkeligt i cybersikkerhed[16]. Forbedring af cybersikkerheden i forsyningskæden bør derfor gennemføres med fokus på SMV'er.

Ud over denne systemiske tilgang kan medlemsstaterne også lægge vægt på indsatser vedrørende cybersikkerhed i specifikke IKT-tjenester og -produkter, der anses for at være særligt vigtige: IKT-teknologier, der anvendes i kritisk informationsinfrastruktur, sikkerhedsmekanismer, der håndhæves i telekommunikationssektoren (kontroller på ISP-niveau...), tillidstjenester som defineret i eIDAS-forordningen og udbydere af cloudcomputing. I sin nationale cybersikkerhedsstrategi for 2019-2024[17]forpligtede Polen sig f.eks. til at udvikle et nationalt system til vurdering og certificering af cybersikkerhed som en mekanisme til kvalitetssikring i forsyningskæden. Dette certificeringssystem vil blive tilpasset EU's certificeringsramme for digitale IKT-produkter, tjenester og processer, der er fastlagt ved EU's forordning om cybersikkerhed (2019/881).

Det er således yderst vigtigt at forbedre cybersikkerheden i forsyningskæden. Dette kan bl.a. opnås ved at indføre stærke politikker til at styrke SMV'er, udsende retningslinjer om

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16]https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

cybersikkerhedskrav i offentlige forvaltningers udbudsbetingelser, fremme samarbejde inden for den private sektor, opbygge OPP'er, fremme mekanismer til koordineret offentliggørelse af sårbarheder (CVD)[18], udarbejde produktcertificeringsordninger, herunder cybersikkerhedskomponenter i digitale initiativer til SMV'er, og finansiere udvikling af færdigheder.

Sikre digital identitet og opbygge tillid til digitale offentlige tjenester

I februar 2020 fremlagde Kommissionen sin vision for EU's digitale omstilling i meddelelsen "Europas digitale fremtid i støbeskeen"[19] med det formål at levere inklusive teknologier, der tjener alle og respekterer EU's grundlæggende værdier. I meddelelsen fremhæves det, at det er afgørende at fremme den digitale omstilling af offentlige forvaltninger i hele Europa. I den henseende er opbygning af tillid til offentlige forvaltninger i forbindelse med digital identitet og tillid til offentlige tjenester af afgørende betydning. Dette er endnu vigtigere i betragtning af, at transaktioner og dataudvekslinger i den offentlige sektor ofte er af følsom karakter.

Mange lande har givet udtryk for, at de har til hensigt at tage fat om dette emne i deres NCSS, heriblandt: Danmark, Estland, Frankrig, Luxembourg, Malta, Spanien, Nederlandene og Det Forenede Kongerige. Nogle af disse lande har givet udtryk for, at dette strategiske mål kan indgå i en mere overordnet plan:

- Estland knytter sin tilhørende handlingsplan om "sikkerhed for elektronisk identitet og elektronisk autentifikationskapacitet" sammen med den overordnede digitale dagsorden 2020 for Estland.
- Af den franske NCSS fremgår det, at ministeren med ansvar for digital teknologi fører tilsyn med udarbejdelsen af en køreplan "til beskyttelse af franskmænds digitale liv, privatliv og personoplysninger".
- Af den nederlandske NCSS fremgår det, at cybersikkerhed i offentlige forvaltninger samt offentlige tjenesteydelser til borgere og virksomheder drøftes mere indgående i den overordnede dagsorden for digital forvaltning.
- Da Det Forenede Kongeriges regering gør stadig flere af sine tjenesteydelser online, har den med støtte fra British National Cybersecurity Centre (NCSC) udpeget regeringens digitale tjeneste (Government Digital Service, GDS) til at sikre, at alle nye digitale tjenesteydelser, der udvikles eller anskaffes af staten, også "som udgangspunkt er sikre".

2.2.3 Andre overvejede strategiske mål

Under ENISA's dokumentationsundersøgelse og de interview, der blev gennemført af ENISA, blev der undersøgt andre strategiske mål. Det blev imidlertid besluttet, at disse mål ikke skulle indgå i rammen for selvvurdering. BILAG C – Andre undersøgte mål

indeholder definitioner af hvert af disse mål, der kan anvendes som input til fremtidige drøftelser af eventuelle forbedringer af en NCSS.

Følgende strategiske mål blev undersøgt med henblik på fremtidige drøftelser:

- Udvikle sektorspecifikke cybersikkerhedsstrategier
- Bekæmpe misinformationskampagner
- Sikre banebrydende teknologier (5G, AI, kvantedatabehandling...)

[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Europas digitale fremtid i støbeskeen, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

- Sikre datasuveræniteten
- Give incitamenter til udvikling af cyberforsikringsbranchen.

2.3 VIGTIGSTE KONKLUSIONER FRA BENCHMARKØVELSEN

Dokumentationsundersøgelsen af eksisterende modenhedsmodeller vedrørende cybersikkerhed blev udført med det formål at indsamle oplysninger og dokumentation til støtte for udformningen af rammen for selvvurdering af national kapacitet i forbindelse med en NCSS. I den forbindelse blev der foretaget en omfattende litteraturgennemgang af eksisterende modeller for at supplere resultaterne fra den indledende screeningsundersøgelse af modenhedsmodeller for cybersikkerhed og eksisterende NCSS, der er udviklet i afsnit 2.1 og 2.2. Denne systematiske gennemgang understøtter udvælgelsen af og begrundelsen for modenhedsniveauer i vurderingsrammen og definitionen af de forskellige dimensioner og indikatorer.

Under den systematiske gennemgang af modenhedsmodeller blev 10 modeller overvejet og analyseret på grundlag af deres vigtigste karakteristika. Den samlede oversigt over de vigtigste karakteristika for hver model, der blev gennemgået inden for rammerne af denne undersøgelse, fremgår af Tabel 2: Oversigt over analyserede modenhedsmodeller, og BILAG A indeholder en mere detaljeret analyse.

Tabel 2: Oversigt over analyserede modenhedsmodeller

Modelnavn	Antal modenhedsniveauer	Antal områder	Vurderingsmetode	Præsentation af resultater
Cybersecurity Capacity Maturity Model for Nations (CMM)	5	5 primære dimensioner	Samarbejde med en lokal organisation om at finjustere modellen, inden den anvendes i national kontekst	Radar med 5 sektioner
Cybersecurity Capability Maturity Model (C2M2)	4	10 primære områder	Metode og værktøjskasse til selvvurdering	Resultattavle med cirkeldiagrammer
Ramme for forbedring af cybersikkerhed i kritisk infrastruktur	Ikke relevant (4 lag)	5 kernefunktioner	Selvvurdering	Ikke relevant
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	5	5 primære områder	Ikke relevant	Ikke relevant
Cybersecurity Maturity Model Certification (CMMC)	5	17 primære områder	Vurdering foretaget af tredjepartsrevisorer	Ikke relevant
Community Cybersecurity Maturity Model (CCSMM)	5	6 primære dimensioner	Vurdering inden for lokalsamfund med input fra statslige og føderale retshåndhævende myndigheder	Ikke relevant
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	5	23 vurderede områder	Ikke relevant	Ikke relevant
Modellen for intern revisionskapacitet (IA- CM) for den offentlige sektor	5	6 elementer	Selvvurdering	Ikke relevant
Globalt indeks for cybersikkerhed (GCI)	Ikke relevant	5 søjler	Selvvurdering	Rangordning

Cyber Power Index (CPI)	Ikke relevant	4 kategorier	Benchmarking foretaget af Economist Intelligence Unit	Prioriteringstabel

Denne systematiske gennemgang gjorde det muligt at drage konklusioner om bedste praksis i eksisterende modeller for at støtte udviklingen af den konceptuelle model til den nuværende modenhedsmodel. Benchmarkøvelsen understøttede navnlig definitionen af modenhedsniveauer, oprettelsen af dimensionsklynger og udvælgelsen af indikatorer samt en hensigtsmæssig metode til visualisering af modellens resultater. De mest relevante resultater for hvert af disse elementer er beskrevet i Tabel 3.

Tabel 3: Vigtigste konklusioner fra benchmarkøvelsen

Element	Vigtigste konklusion
Modenhedsniveauer	▶ Generelt anses en modenhedsskala med fem niveauer for rammer for vurdering af cybersikkerhedskapacitet for at være passende og i stand til at give detaljerede vurderingsresultater (se Tabel 6 Sammenligning af løbetidsniveauer for et udtømmende overblik over definitionen af modenhedsniveauer for hver model) ▶ Alle modeller giver en kvalificeret definition af hvert modenhedsniveau, som efterfølgende tilpasses de forskellige dimensioner eller klynger af dimensioner ▶ Ved måling af en cybersikkerhedskapacitets modenhed vurderes normalt to primære aspekter: strategiernes modenhed og modenheden af de processer, der er indført for at gennemføre strategierne.
Attributter	▶ Den komparative analyse af egenskaberne ved eksisterende modenhedsmodeller viser heterogene resultater med i gennemsnit fire og fem attributter pr. model ▶ En model, der er baseret på omkring fire eller fem attributter, giver landene det rette datadetaljeringsniveau ved at gruppere relevante dimensioner og sikre resultaternes læsbarhed (se Tabel 7: Sammenligning af attributter/dimensionerbeskrivelsen af attributterne for hver model) ▶ Det centrale princip, der anvendes i alle modeller til definition af klyngerne, er baseret på sammenhængen mellem elementer, der er grupperet inden for hver klynge.
Vurderingsmetode	▶ Der er stor forskel på de vurderingsmetoder, der anvendes i de forskellige analyserede modeller ▶ Den mest udbredte vurderingsmetode er baseret på selvvurdering.
Præsentation af resultater	▶ Det er vigtigt at opdele resultaterne efter de forskellige detaljeringsniveauer ▶ Visualiseringsmetoden bør være selvforklarende og letlæselig.

Den konceptuelle model var baseret på benchmarkingøvelsen med de forskellige modenhedsmodeller samt på ENISA's tidligere arbejde. Det blev også besluttet at bygge videre på *ENISA's interaktive onlineredskab* til udvikling af de modenhedsindikatorer, der anvendes til hver enkelt attribut.

2.4 UDFORDRINGER I FORBINDELSE MED NCSS-EVALUERINGEN

Medlemsstaterne står over for mange udfordringer, når de skal opbygge cybersikkerhedskapacitet, og mere specifikt når de skal sikre, at deres kapacitet er opdateret med den seneste udvikling. Nedenfor findes en oversigt over de udfordringer, medlemsstaterne registrerede og drøftede som led i denne undersøgelse:

- **Vanskeligheder i forbindelse med koordinering og samarbejde:** Koordinering af tiltag vedrørende cybersikkerhed på nationalt plan for at have en effektiv respons på

problemer med cybersikkerhed kan vise sig at være en udfordring på grund af de mange involverede interessenter.

- **Manglende ressourcer til at udføre vurderingen:** Afhængigt af den lokale kontekst og den nationale forvaltningsstruktur for cybersikkerhed kan det eventuelt kræve mere end 15 manddage at evaluere NCSS'en og dens mål.
- **Manglende støtte til udvikling af cybersikkerhedskapacitet:** Nogle medlemsstater var enige om, at de for at godkende et budget og få støtte til at udvikle cybersikkerhedskapacitet først blev nødt til at gennemføre en evalueringsfase for at identificere mangler og begrænsninger.
- **Vanskeligheder med at tilføre strategien succeser eller ændre den:** Eftersom trusler udvikler sig dagligt, og teknologien forbedres, skal handlingsplanerne løbende tilpasses. Det er imidlertid fortsat en vanskelig opgave at evaluere en NCSS og ændre selve strategien. Det gør det igen vanskeligt at identificere begrænsninger og mangler i en NCSS.
- **Vanskeligheder med at måle effektiviteten af en NCSS:** Der kan indsamles parametre til måling af forskellige områder såsom fremskridt, gennemførelse, modenhed og effektivitet. Det er forholdsvis let at måle fremskridt og gennemførelse sammenlignet med måling af effektivitet, omend sidstnævnte stadig er den mest relevante for evalueringen af resultaterne og virkningerne af en NCSS. På grundlag af de interview, der blev gennemført af ENISA, anførte et stort antal medlemsstater, at det er vigtigt kvantitativt at måle effektiviteten af en NCSS, men at det også er en meget krævende opgave, som i nogle tilfælde er ret umulig.
- **Vanskeligheder ved at vedtage en fælles ramme:** EU's medlemsstater opererer i forskellige sammenhænge med hensyn til politik, organisationer, kultur, samfundsstruktur og modenhed af deres NCSS'er. Visse medlemsstater, der blev interviewet som led i denne undersøgelse, gav udtryk for, at det kan være vanskeligt at forsvare og anvende en selvvurderingsramme, der passer alle.

2.5 FORDELE VED EN NATIONAL KAPACITETSVURDERING

Alle EU-medlemsstater har siden 2017 haft en NCSS[20]. Dette er en positiv udvikling, men det er også vigtigt, at medlemsstaterne er i stand til at foretage en korrekt vurdering af disse NCSS'er og dermed øge værdien af deres strategiske planlægning og gennemførelse.

Et af målene for vurderingsrammen for national kapacitet er at vurdere cybersikkerhedskapaciteten på grundlag af de prioriteter, der er fastsat i de forskellige NCSS'er. Rammen vurderer grundlæggende niveauet af modenhed for medlemsstaternes cybersikkerhedskapacitet på de områder, der er fastsat i de forskellige NCSS'er. Resultaterne af rammen hjælper således medlemsstaternes politiske beslutningstagere med at definere den nationale strategi for cybersikkerhed ved at give dem oplysninger om situationen i de enkelte lande[21]. Formålet med NCAF'en er i sidste ende at hjælpe medlemsstaterne med at identificere områder, hvor der kan ske forbedringer, og opbygge kapacitet.

Formålet med rammen er at tilbyde medlemsstaterne en selvvurdering af deres modenhed ved at vurdere deres NCSS-mål, hvilket vil hjælpe dem med at styrke og opbygge kapacitet inden for cybersikkerhed, både på strategisk og operationelt plan.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

På et mere praktisk plan og baseret på de interview, som ENISA har gennemført med flere agenturer, der er ansvarlige for cybersikkerhed i de enkelte medlemsstater, blev følgende fordele ved vurderingsrammen for national kapacitet identificeret og fremhævet:

- Give nyttige oplysninger til udvikling af en langsigtet strategi (f.eks. god praksis, retningslinjer)
- Bidrage til at identificere manglende elementer i NCSS'erne
- Bidrage til yderligere opbygning af cybersikkerhedskapacitet
- Understøtte ansvarligheden af politiske tiltag
- Skabe troværdighed over for offentligheden og internationale partnere
- Støtte opsøgende arbejde og styrke dets omdømme i offentligheden som en gennemsigtig organisation
- Bidrage til at foregribe fremtidige problemstillinger
- Bidrage til at identificere indhøstede erfaringer og bedste praksis
- Definere en basislinje for cybersikkerhedskapaciteten i hele EU for at lette drøftelser
- Bidrage til at evaluere den nationale kapacitet inden for cybersikkerhed.

3. METODE I RAMMEN FOR VURDERING AF NATIONAL KAPACITET

3.1 GENERELT FORMÅL

Hovedformålet med NCAF'en er at måle niveauet af modenhed for**medlemsstaternes** cybersikkerhedskapacitet for at hjælpe dem med at foretage en evaluering af deres nationale cybersikkerhedskapacitet, øge bevidstheden om landets modenhedsniveau, identificere områder, hvor der kan ske forbedringer, og opbygge cybersikkerhedskapacitet.

3.2 MODENHEDSNIVEAUER

Rammen er baseret på **fem modenhedsniveauer**, der definerer de faser, som medlemsstaterne gennemgår, når de opbygger deres cybersikkerhedskapacitet på det område, der er omfattet af hvert NCSS-mål. Niveauerne repræsenterer stigende modenhed fra det indledende **niveau 1**, hvor medlemsstaterne ikke har en klart defineret tilgang til opbygning af cybersikkerhedskapacitet på de områder, der er omfattet af NCSS-målene, til det øverste **niveau 5**, hvor strategien for opbygning af cybersikkerhedskapacitet er dynamisk og tilpasset miljøudviklingen. Tabel 4 viser skalaen for modenhedsniveauet med en beskrivelse af hvert modenhedsniveau.

Tabel 4: ENISA's ramme for vurdering af national kapacitet med fem modenhedsniveauer

NIVEAU 1 – INDLEDENDE/AD HOC	NIVEAU 2 – TIDLIG DEFINITION	NIVEAU 3 – ETABLERING	NIVEAU 4 – OPTIMERING	NIVEAU 5 – TILPASNINGSEGNE T
Medlemsstaten har ikke en klart defineret tilgang til kapacitetsopbygning inden for cybersikkerhed på de områder, der er omfattet af NCSS-målene. Landet kan dog have vedtaget nogle generelle mål og have gennemført nogle undersøgelser (tekniske, politiske) for at forbedre den nationale kapacitet.	Der er fastlagt en national tilgang til kapacitetsopbygning på det område, der er omfattet af NCSS-målene. De handlingsplaner eller aktiviteter, der skal levere resultaterne, er indført, men er i en tidlig fase. Desuden kan aktive interessenter være blevet identificeret og/eller inddraget.	Handlingsplanen for kapacitetsopbygning på det område, der er omfattet af NCSS-målene, er klart defineret, og de berørte parter bakker op om den. Praksis og aktiviteter håndhæves og gennemføres ensartet på nationalt plan. Aktiviteterne er defineret og dokumenteret med klar ressourceallokering og -styring samt et sæt frister.	Handlingsplanen vurderes regelmæssigt: den er prioriteret, optimeret og bæredygtig. Resultaterne af kapacitetsopbygge nde cybersikkerhedsak tiviteter måles regelmæssigt. Succesfaktorer, udfordringer og mangler i gennemførelsen af aktiviteterne registreres.	Strategien for kapacitetsopbygning inden for cybersikkerhed er dynamisk og fleksibel. Konstant fokus på udvikling i miljøet (teknologiske fremskridt, globale konflikter, nye trusler osv.) styrker evnen til at træffe hurtige beslutninger og handle hurtigt med henblik på forbedring.

3.3 KLYNGER OG DEN OVERORDNEDE STRUKTUR I SELVVURDERINGSRAMMEN

Selvvurderingsrammen består af **fire klynger**: (I) Forvaltning af og standarder for cybersikkerhed, (II) Kapacitetsopbygning og bevidsthed, (III) Love og administrative bestemmelser, og (IV) Samarbejde. Hver af disse klynger dækker et centralt tematisk område for opbygning af cybersikkerhedskapacitet i et land og indeholder en pulje af forskellige mål, som medlemsstaterne kan medtage i deres NCSS. Navnlig:

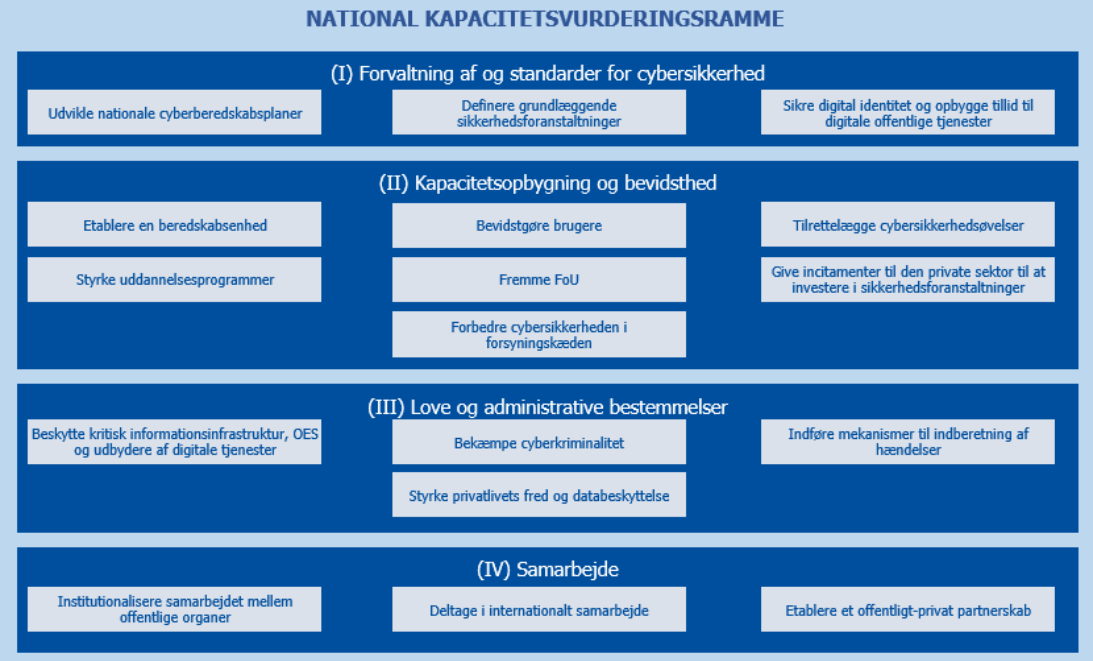
- **(I) Forvaltning af og standarder for cybersikkerhed**: Denne klynge måler medlemsstaternes evne til at indføre relevant forvaltning, standarder og god praksis på cybersikkerhedsområdet. Denne dimension tager højde for forskellige aspekter af cyberforsvar og modstandsdygtighed og støtter samtidig udviklingen af den nationale cybersikkerhedsindustri og opbygning af tillid til regeringerne.
- **(II) Kapacitetsopbygning og bevidsthed**: Denne klynge vurderer medlemsstaternes evne til at øge bevidstheden om cybersikkerhedsrisici og -trusler og om, hvordan de skal håndteres. Desuden måler denne dimension landets evne til løbende at opbygge sin cybersikkerhedskapacitet og øge det overordnede videns- og færdighedsniveau på dette område. Den omhandler udvikling af markedet for cybersikkerhed samt fremskridt i FoU inden for cybersikkerhed. Denne klynge omgrupperer alle de mål, der udgør fundamentet for at fremme kapacitetsopbygning.
- **(III) Love og administrative bestemmelser**: Denne klynge måler medlemsstaternes kapacitet til at indføre de nødvendige love og administrative instrumenter til at håndtere og bekæmpe stigningen i cyberkriminalitet og beslægtede cyberhændelser samt beskytte kritisk informationsinfrastruktur. Derudover vurderer denne dimension medlemsstaternes kapacitet til at oprette en retlig ramme for beskyttelse af borgere og virksomheder, hvis det f.eks. skulle blive nødvendigt at afveje sikkerhed og privatlivets fred.
- **(IV) Samarbejde**: Denne klynge evaluerer samarbejdet og informationsudvekslingen mellem forskellige interessentgrupper på nationalt og internationalt plan som et vigtigt redskab til bedre at forstå og reagere på et trusselsmiljø i konstant forandring.

De mål, der indgår i modellen, er dem, der i vid udstrækning vedtages af medlemsstaterne, og de er blevet udvalgt blandt de mål, der er anført i afsnit 2.2. Modellen vurderer navnlig følgende mål:

- 1. Udvikle nationale cyberberedskabsplaner (I)
- 2. Opstille grundlæggende sikkerhedsforanstaltninger (I)
- 3. Sikre digital identitet og opbygning af tillid til digitale offentlige tjenester (I)
- 4. Oprette en beredskabsenhed (II)
- 5. Bevidstgøre brugere (II)
- 6. Tilrettelægge cybersikkerhedsøvelser (II)
- 7. Styrke uddannelsesprogrammer (II)
- 8. Fremme FoU (II)
- 9. Give incitamenter til den private sektor til at investere i sikkerhedsforanstaltninger (II)
- 10. Forbedre cybersikkerheden i forsyningskæden (II)
- 11. Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester (III)
- 12. Bekæmpe cyberkriminalitet (III)
- 13. Indføre mekanismer til indberetning af hændelser (III)
- 14. Styrke privatlivets fred og databeskyttelse (III)
- 15. Institutionalisere samarbejdet mellem offentlige agenturer (IV)
- 16. Deltage i internationalt samarbejde (IV)
- 17. Etablere et offentlig-privat partnerskab (IV)

De fire klynger og de underliggende mål kombineres i modellen for at få et helhedsbillede af modenheden af medlemsstaternes cybersikkerhedskapacitet. Figur 1 viser den overordnede struktur i rammen for selvvurdering og viser, hvordan disse elementer, dvs. mål, klynger og selvvurderingsrammer, er knyttet til vurderingen af et lands resultater.

Figur 1: Opbygning af selvvurderingsrammen



For hvert mål, der indgår i selvvurderingsrammen, er der en række indikatorer fordelt på de fem modenhedsniveauer. Hver indikator er baseret på et ja/nej-spørgsmål. Indikatoren kan være obligatorisk eller frivillig.

3.4 SCORINGSMEKANISME

Scoringsmekanismen i rammen for selvvurdering tager højde for ovennævnte elementer og de principper, der er anført i afsnit 3.5. Modellen genererer en score baseret på værdien af to parametre, **modenhedsniveauet** og **dækningsniveauet**. Hvert parameter kan beregnes på forskellige niveauer: i) pr. mål, ii) pr. klynge af mål eller iii) generelt.

Score på objektivt niveau

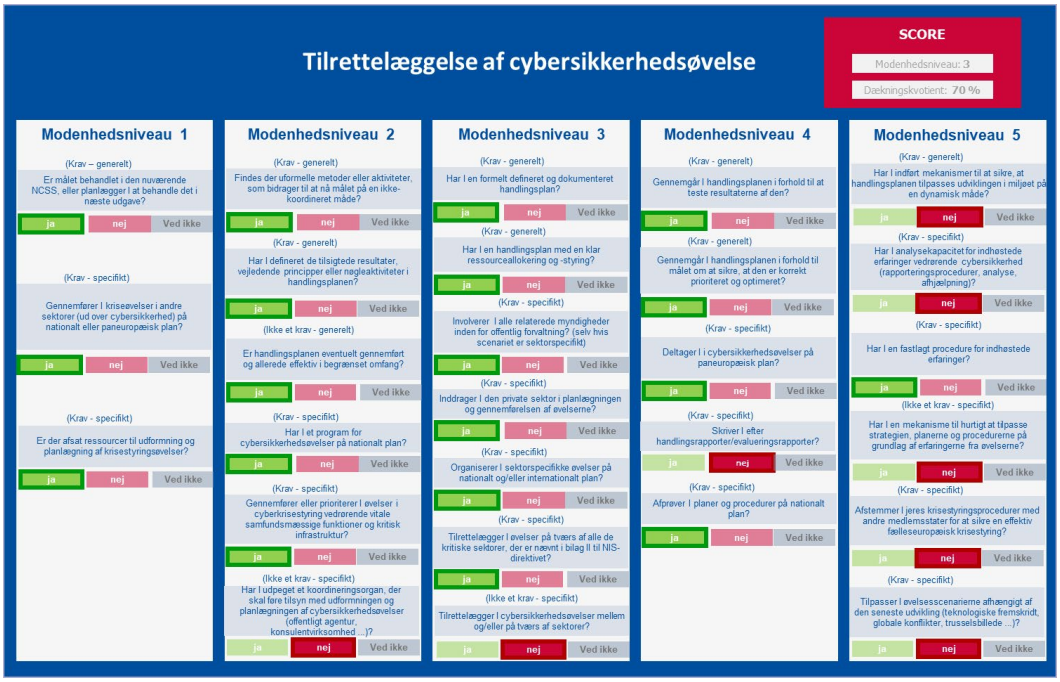
Score for modenhedsniveau giver et overblik over modenhedsniveauet ved at vise, hvilken kapacitet og praksis der var indført. Scoren for modenhedsniveau beregnes som det højeste niveau, for hvilket respondenten opfyldte alle kravene (*dvs.* svaret på alle obligatoriske spørgsmål var JA), samt at alle krav på forrige modenhedsniveauer var opfyldt.

Dækningsniveauet viser omfanget af dækningen af alle de indikatorer, for hvilke svaret er positivt, uanset deres niveau. Det er en supplerende værdi, der tager højde for alle de indikatorer, der måler et mål. Dækningsgraden beregnes som forholdet mellem det samlede antal spørgsmål inden for målet og antal spørgsmål, hvor svaret er positivt.

Det er vigtigt at præcisere, at ordet ***score*** i resten af dokumentet henviser til værdien af både modenhedsniveauet og dækningsgraden.

Figur 2 – Scoringsmekanismen pr. mål er en visualisering af den evalueringsmekanisme, der er beskrevet i afsnit 3.1, og som vil blive præciseret yderligere nedenfor.

Figur 2: Scoringsmekanisme pr. mål



Figur 2 viser et eksempel på, hvordan modenhedsniveauet beregnes efter mål. Det er værd at bemærke, at respondenten opfyldte alle kravene til de tre første modenhedsniveauer og kun delvist opfyldte kravene på niveau 4. Scoren viser derfor, at ***respondentens modenhedsniveau erniveau 3 for målet "Tilrettelæggelse af cybersikkerhedsøvelser"****.*

I det eksempel, der er vist i Figur 2, er det i modenhedsniveauet for målet imidlertid muligt at registrere oplysningerne fra de indikatorer, der har en positiv score, og som ligger over niveau 3. I dette tilfælde kan dækningsgraden give et overblik over alle de elementer, som respondenten har gennemført for at nå dette mål, til trods for det faktiske modenhedsniveau. I dette tilfælde er forholdet mellem det samlede antal spørgsmål inden for målet og antal spørgsmål, hvor svaret er positivt, 19/27, dvs. ***at dækningsgraden er 70 %.***

For at være tilpasset de særlige forhold i medlemsstaterne og samtidig give mulighed for en ensartet oversigt, beregnes scoren ud fra to forskellige stikprøver på klyngeniveau og det overordnede niveau:

- **Generelle scorer:** En komplet stikprøve, der dækker alle de mål, der er medtaget i klyngen eller inden for den overordnede ramme (fra 1 til 17).
- **Specifikke scorer:** Én specifik stikprøve, der kun dækker de mål, som medlemsstaten har udvalgt (normalt svarende til målene i det pågældende lands NCSS) inden for klyngen eller den overordnede ramme.

Scorer på klyngeniveau

Det **generelle modenhedsniveau for hver klynge** beregnes som det aritmetiske gennemsnit af modenhedsniveauet for alle målene i den pågældende klynge.

Det **specifikke modenhedsniveau for hver klynge** beregnes som det aritmetiske gennemsnit af modenhedsniveauet for målene inden for den klynge, som medlemsstaten valgte at vurdere (de svarer normalt til målene i det pågældende lands NCSS).

F.eks. viser Figur 1, at klyngen (I) forvaltning af og standarder for cybersikkerhed består af tre mål. Hvis det antages, at respondenten valgte kun at vurdere de to første mål, men ikke det tredje, og hvis det antages, at de to første mål havde et modenhedsniveau på henholdsvis 2 og 4, er klyngens modenhedsniveau, når alle målene tages i betragtning, niveau 2 (klynge (I) generelt modenhedsniveau = (2 + 4)/3), hvorimod klyngens modenhedsniveau, hvis kun de specifikke mål, som den ansvarlige for vurderingen har valgt, tages i betragtning, er niveau 3 (klynge (I) specifikt modenhedsniveau = (2 + 4)/2).

Den **generelle dækningsgrad for hver klynge** beregnes som forholdet mellem det samlede antal spørgsmål inden for klyngen og antal spørgsmål, hvor svaret er positivt.

Den **specifikke dækningsgrad for hver klynge** beregnes som forholdet mellem det samlede antal spørgsmål i klyngen, der vedrører mål, som medlemsstaten valgte at vurdere (hvilket normalt svarer til målene i det pågældende lands NCSS), og antallet af spørgsmål, for hvilke svaret er positivt.

Scorer på overordnet niveau

Et lands overordnede generelle modenhedsniveau beregnes som det aritmetiske gennemsnit af modenhedsniveauet for alle målene i rammen, fra ét til 17.

Et lands specifikke modenhedsniveau beregnes som det aritmetiske gennemsnit af modenhedsniveauet for målene inden for den ramme, som medlemsstaten valgte at vurdere (den svarer normalt til målene i det pågældende lands NCSS).

Et lands overordnede generelle dækningsgrad beregnes som forholdet mellem det samlede antal spørgsmål inden for de mål, der er medtaget i rammen (fra 1 til 17) og antal spørgsmål, hvor svaret er positivt.

Et lands overordnede specifikke dækningsgrad beregnes som forholdet mellem det samlede antal spørgsmål inden for målene i den ramme, som medlemsstaten valgte at vurdere (som normalt svarer til målene i det pågældende lands NCSS), og antallet af spørgsmål, for hvilke svaret er positivt.

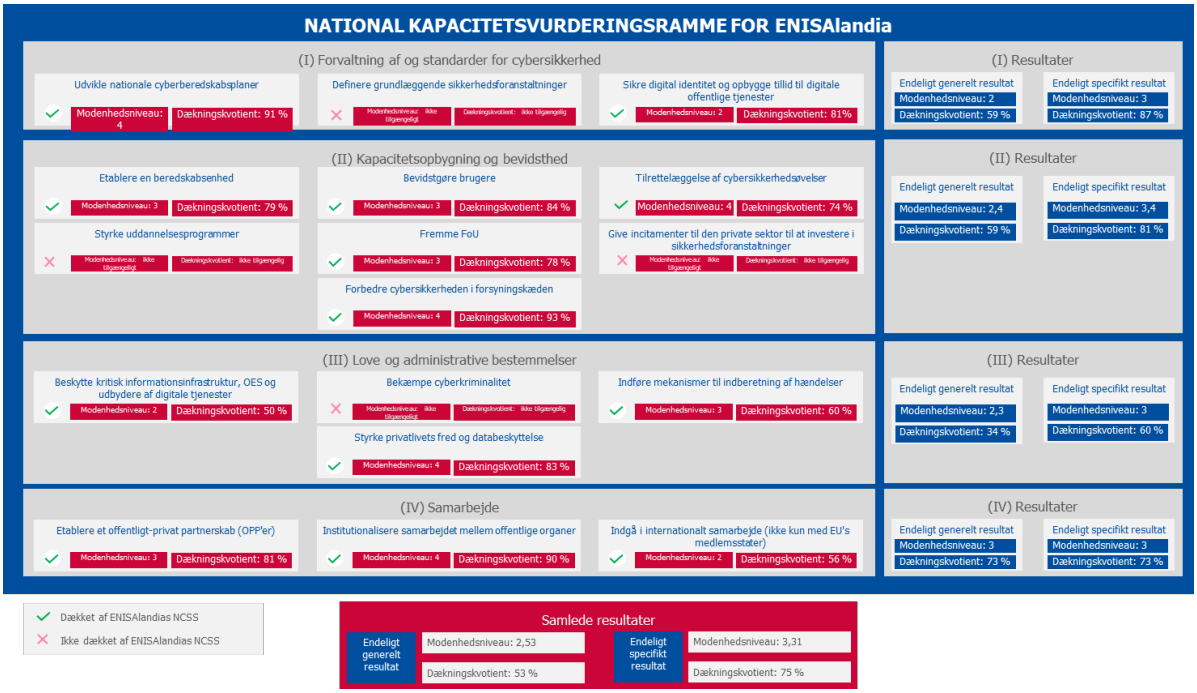
For hver indikator kan respondenterne vælge en tredje svarmulighed "ved ikke/ikke relevant". I dette tilfælde indgår indikatoren ikke i den samlede beregning af resultaterne.

Modenhedsniveauerne på klyngeniveau og overordnet niveau beregnes med et aritmetisk gennemsnit for at vise fremskridtene mellem to vurderinger. Alternativet, dvs. beregning af klyngens modenhedsniveau og det samlede modenhedsniveau som det mindst udviklede måls modenhedsniveau, kan – omend det er relevant ud fra et modenhedssynspunkt – ikke tage højde for de fremskridt, der er gjort på områder, som er omfattet af andre mål.

Da klyngeniveauet og det overordnede niveau er konsolideret med henblik på rapportering, har man valgt at anvende det aritmetiske gennemsnit. Hvis der ønskes en højere nøjagtighed, anvendes scorerne på objektivt niveau til rapporteringsformål.

Figur 3 nedenfor opsummerer scoringsmekanismerne på modellens forskellige niveauer (mål, klynge, samlet).

Figur 3: Samlet scoringsmekanisme



3.5 KRAV TIL SELVVURDERINGSRAMMEN

Den ramme for vurdering af national kapacitet, der præsenteres i dette afsnit, er baseret på de behov, som medlemsstaterne har fremhævet, og den er bygget op omkring en række krav, der er anført nedenfor:

- NCAF'en anvendes på frivillig basis af medlemsstaten som en ramme for selvvurdering
- NCAF'en har til formål at måle medlemsstaternes cybersikkerhedskapacitet med hensyn til de 17 mål. Medlemsstaten kan dog vælge de mål, den ønsker at vurdere i forhold til, og vælge kun at vurdere en undergruppe af de 17 mål.
- Rammen for selvvurdering har til formål at måle niveauet af modenhed for medlemsstatens cybersikkerhedskapacitet.
- Resultaterne af vurderingen offentliggøres ikke, medmindre medlemsstaten på eget initiativ beslutter at gøre det.
- Medlemsstaten kan vise vurderingsresultaterne ved at fremlægge modenhedsniveauet for landets cybersikkerhedskapacitet i en klynge af målsætninger eller endda for et enkelt mål.
- Alle vurderede mål er lige relevante inden for vurderingsrammen, og de har derfor samme betydning. Det samme gælder for de indikatorer, der anvendes inden for den.
- Medlemsstaten har mulighed for at følge sine fremskridt over tid.

Rammen for selvvurdering har til formål at støtte medlemsstaterne i opbygningen af cybersikkerhedskapacitet, og den omfatter derfor også en række anbefalinger eller retningslinjer, der skal vejlede de europæiske lande med hensyn til at forbedre deres modenhed.

Bemærk: disse anbefalinger eller retningslinjer er generelle og er baseret på ENISA's publikationer samt erfaringer fra andre lande og vil være baseret på resultatet af selvvurderingen.

4. NCAF-INDIKATORER

4.1 RAMMEINDIKATORER

I dette afsnit præsenteres indikatorerne for ENISA's ramme for vurdering af national kapacitet. De følgende sektioner er opdelt efter klynge.

For hver klynge viser en tabel det omfattende sæt indikatorer i form af spørgsmål, der er repræsentative for et bestemt modenhedsniveau. Spørgeskemaet er det vigtigste instrument til selvvurderingen. For hvert mål er der to sæt indikatorer, der skal noteres:

- Et sæt generelle strategiske spørgsmål vedrørende modenhed (9 generelle spørgsmål), der er markeret fra "(a)" til "(c)" for hvert modenhedsniveau og gentaget for hvert mål og
- Et sæt spørgsmål om cybersikkerhed (319 spørgsmål om cybersikkerhedskapacitet), der er nummereret fra "1" til "10" for hvert modenhedsniveau, der er specifikt for det område, der er omfattet af målet.

Hvert spørgsmål er markeret med et mærke (0-1), der angiver, om spørgsmålet er en obligatorisk indikator (1) eller en frivillig indikator (0) for modenhedsniveauet.

Hvert spørgsmål kan identificeres ved hjælp af et identifikationsnummer bestående af:

- målets nummer
- modenhedsniveauet
- spørgsmålets nummer.

Spørgsmål med ID 1.2.4 er f.eks. det fjerde spørgsmål i modenhedsniveau 2 for det strategiske mål (I) "Udvikling af nationale cyberberedskabsplaner".

Det skal bemærkes, at spørgsmålene i hele spørgeskemaet er på nationalt plan, medmindre andet er angivet. I alle spørgsmål henviser pronomenet "I" til medlemsstaten som helhed og henviser ikke til det individuelle eller statslige organ, der foretager vurderingen.

Der er en definition af hvert mål i kapitel 2.2 – Fælles mål, der er fastlagt inden for rammerne af den europæiske NCSS.

4.1.1 Gruppe nr. 1: Forvaltning af og standarder for cybersikkerhed

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
1 – Udvikle nationale cyberberedskabsplaner	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Begyndte I at udarbejde nationale cyberberedskabsplaner, *f.eks.* ved at fastsætte beredskabsplanernes generelle mål, anvendelsesområde og/eller principper osv.?	1	Har I en doktrin/national strategi, der omfatter cybersikkerhed som en krisefaktor (dvs. en plan, en politik osv.)?	1	Har I en cyberkrisestyringsplan på nationalt plan?	1	Er I tilfredse med antallet eller procentdelen af kritiske sektorer, der er medtaget i den nationale cyberberedskabsplan?	1	Har I indført en procedure for indhøstning af erfaringer efter cyberøvelser eller faktiske kriser på nationalt plan?	1
	2	Er den almindelige opfattelse, at cyberhændelser udgør en krisefaktor, der kan true den nationale sikkerhed?	0	Har I et knudepunkt til at indhente oplysninger og informere beslutningstagere, *dvs.* metoder, platforme eller steder, der sikrer, at alle kriseaktionsaktører har adgang til de samme realtidsoplysninger om cyberkrisen?	1	Har I cyberkrisespecifikke procedurer på nationalt plan?	1	Organiserer I tilstrækkeligt ofte aktiviteter (dvs. øvelser) vedrørende den nationale cyberberedskabsplanlægning?	1	Har I en proces til regelmæssigt at teste den nationale plan?	1
	3	Er der foretaget undersøgelser (tekniske, operationelle, politiske) inden for cyberberedskabsplanlægning?	0	Er der afsat relevante ressourcer til at føre tilsyn med udviklingen og gennemførelsen af nationale cyberberedskabsplaner?	1	Har I et kommunikationsteam, der er specielt uddannet til at reagere på cyberkriser og informere offentligheden?	1	Er der tilstrækkeligt mange mennesker, der beskæftiger sig med kriseplanlægning, ser på de indhøstede erfaringer og gennemfører ændringer?	1	Har I passende værktøjer og platforme til at opbygge situationskendskab?	1
	4	-		Har I en metode til vurdering af cybertrusler på nationalt plan, som omfatter procedurer for konsekvensanalyse?	0	Inddrager I alle relevante nationale interessenter (national sikkerhed, forsvar, civilbeskyttelse, retshåndhævelse, ministerier, myndigheder osv.)?	1	Har I tilstrækkeligt mange mennesker, der er uddannet til at reagere på cyberkriser på nationalt plan?	1	Følger I en specifik modenhedsmodel til at overvåge og forbedre cyberberedskabsplanen?	0
	5	-		-		Har I passende krisestyringsfaciliteter og situationsrum?	1	-		Har I ressourcer, der enten er specialiseret i foregribelse af trusler eller arbejde med fremtidig cybersikkerhed med henblik på at afværge kommende kriser eller fremtidens udfordringer?	0

	6	-		-		Inddrager I internationale interessenter i EU, hvis det er nødvendigt?	0	-		-	
	7	-		-		Inddrager I internationale interessenter i lande uden for EU, hvis det er nødvendigt?	0	-		-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
2 – Definere grundlæggende sikkerhedsforanstaltninger	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen med hensyn til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I gennemført en undersøgelse for at identificere krav og mangler for **offentlige** organisationer baseret på internationalt anerkendte standarder, *f.eks.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS osv.?	1	Er sikkerhedsforanstaltningerne truffet i overensstemmelse med internationale/nationale standarder?	1	Er grundlæggende sikkerhedsforanstaltninger obligatoriske?	1	Er der en procedure for hyppig opdatering af grundlæggende sikkerhedsforanstaltninger?	1	Har I en proces til at forstærke IKT, når hændelser ikke er omfattet af foranstaltningerne?	1
	2	Har I gennemført en undersøgelse for at identificere krav og mangler for **offentlige** organisationer baseret på internationalt anerkendte standarder, f.eks. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS osv.?	1	Høres den private sektor og andre interessenter i forbindelse med fastlæggelsen af grundlæggende sikkerhedsforanstaltninger?	1	Gennemfører I horisontale sikkerhedsforanstaltninger på tværs af kritiske sektorer?	1	Findes der en overvågningsmekanisme til at undersøge udbredelsen af grundlæggende sikkerhedsforanstaltninger?	1	Vurderer I relevansen af nye standarder, der er udviklet som reaktion på den seneste udvikling i trusselsbilledet?	1
	3	-		-		Gennemfører I sektorspecifikke sikkerhedsforanstaltninger på tværs af kritiske sektorer?	1	Findes der en national myndighed til at kontrollere, om grundlæggende sikkerhedsforanstaltninger håndhæves?	1	Har eller fremmer I en national procedure for koordineret offentliggørelse af sårbarheder?	1

	4	-				Er grundlæggende sikkerhedsforanstaltninger i overensstemmelse med relevante certificeringsordninger?	1	Har I indført en procedure til at udpege organisationer, der ikke opfylder kravene inden for et bestemt tidsrum?	1	-	
	5	-		-		Er der indført en selvvurderingsprocedure for grundlæggende sikkerhedsforanstaltninger?	1	Findes der en revisionsprocedure til at sikre, at sikkerhedsforanstaltningerne anvendes korrekt?	1	-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
2 – Definition af grundlæggende sikkerhedsforanstaltninger	6	-		-		Gennemgår I de obligatoriske grundlæggende sikkerhedsforanstaltninger i forbindelse med offentlige organers indkøb?	0	Fastlægger eller tilskynder I aktivt til vedtagelse af sikre standarder for udvikling af kritiske IT-/OT-produkter (medicinsk udstyr, opkoblede og selvkørende køretøjer, professionelt radioudstyr, tungt industriudstyr osv.)?	0	-	

NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
3 – Sikre digital identitet og opbygge tillid til digitale offentlige tjenester	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I gennemført undersøgelser eller mangelanalyser for at afgrænse behovet for at sikre digitale offentlige tjenester til borgere og virksomheder?	1	Foretager I risikoanalyser for at afgøre aktivernes eller tjenesternes risikoprofil, inden de flyttes til skyen, eller for at anvende projekter til digital omstilling?	1	Fremmer I metoder til "privacy-by-design" i alle e-forvaltningsprojekter?	1	Indsamler I indikatorer for cybersikkerhedshændelser, der omfatter brud på digitale offentlige tjenester?	1	Deltager I i europæiske arbejdsgrupper for at opretholde standarder og/eller udforme nye krav til elektroniske tillidstjenester (e-signaturer, e-segl, e-registrerede leveringstjenester, tidsstempling, webstedsautentifikation), f.eks. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU osv.?	1

	2	-		Har I en strategi for at opbygge eller fremme sikre nationale elektroniske identifikationsordninger (eID'er) for borgere og virksomheder?	1	Inddrager I private interessenter i udformningen og leveringen af sikre digitale offentlige tjenester?	1	Har I gennemført gensidig anerkendelse af elektroniske identifikationsmidler med andre medlemsstater?	1	Deltager I aktivt i peerevalueringer som led i en anmeldelse af eID-ordninger til Europa-Kommissionen?	1
	3	-		Har I en strategi for at opbygge eller fremme sikre nationale elektroniske tillidstjenester (e-signaturer, e-segl, e-registrerede leveringstjenester, tidsstempling, webstedsautentifikation) for borgere og virksomheder?	1	Implementerer I et minimumsniveau for sikkerheden for alle digitale offentlige tjenester?	1	-		-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
3 – Sikre digital identitet og opbygge tillid til digitale offentlige tjenester	4	-		Har I en strategi for statslig cloudcomputing (en cloudcomputing-strategi rettet mod statslige og offentlige organer, såsom ministerier, statslige agenturer og offentlige forvaltninger osv.), som tager højde for konsekvenser for sikkerheden?	0	Findes der nogen elektroniske identifikationsordninger for borgere og virksomheder med et betydeligt eller højt sikringsniveau som defineret i bilaget til eIDAS-forordning (EU) nr. 910/2014?	1	-		-	
	5	-		-		Har I digitale offentlige tjenester, der kræver elektroniske identifikationsordninger med et betydeligt eller højt sikringsniveau som defineret i bilaget til eIDAS-forordning (EU) nr. 910/2014?	1	-		-	
	6	-		-		Har I udbydere af tillidstjenester for borgere og virksomheder (e-signaturer, e-segl, e-registrerede leveringstjenester, tidsstempling, webstedsautentifikation)?	1	-		-	
	7	-		-		Tilskynder I til vedtagelsen af grundlæggende sikkerhedsforanstaltninger for alle modeller for udbredelse af cloudcomputing (f.eks. private, offentlige og hybride modeller? IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Gruppe nr. 2: Kapacitetsopbygning og bevidsthed

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
4 – Etablere en beredskabsenhed	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I uformel beredskabskapacitet, der administreres inden for eller mellem den offentlige og den private sektor?	1	Har I mindst én officiel national CSIRT?	1	Har I beredskabskapacitet for de sektorer, der er nævnt i bilag II til NIS-direktivet?	1	Har I defineret og fremmet standardiseret praksis for beredskabsprocedurer og systemer til klassificering af hændelser?	1	Har I en mekanisme til tidlig opdagelse, identifikation, forebyggelse, reaktion og afhjælpning af nuldagssårbarheder?	1
	2	-		Har jeres nationale CSIRT('er) et klart defineret interventionsområde, f.eks. afhængigt af den sektor, der rammes, hændelsestype, konsekvenser?	1	Findes der i jeres land en CSIRT-samarbejdsmekanisme til at reagere på hændelser?	1	Evaluerer I jeres beredskabskapacitet for at sikre, at I har tilstrækkelige ressourcer og færdigheder til at udføre de opgaver, der er fastsat i punkt (2) i bilag I til NIS-direktivet?	1	-	
	3	-		Er der klart definerede forbindelser mellem jeres nationale CSIRT('er) og andre nationale interessenter vedrørende det nationale cybersikkerhedslandskab og beredskabspraksis (f.eks. retshåndhævende myndigheder, militæret, internetudbydere, NCSC)?	0	Er beredskabskapaciteten i jeres nationale CSIRT('er) i overensstemmelse med bilag I til NIS-direktivet, *dvs.* tilgængelighed, fysisk sikkerhed, driftskontinuitet, internationalt samarbejde, overvågning af hændelser, kapacitet til tidlig varsling og advarsler, beredskab, risikoanalyse og situationsrapporter, samarbejde med den private sektor, standardpraksis osv.?	1	-		-	
	4	-				Findes der en samarbejdsmekanisme med andre nabolande om hændelser?	1	-		-	

	5	-		-		Har I formelt defineret klare politikker og procedurer for håndtering af hændelser?	1	-		-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
4 – Etablere en beredskabsenhed	6	-		-		Deltager jeres nationale CSIRT('er) i cybersikkerhedsøvelser på både nationalt og internationalt plan?	1	-		-	
	7	-		-		Er jeres nationale CSIRT('er) tilknyttet FIRST (forum for enheder, der håndterer sikkerhedshændelser)?	0	-		-	

NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
5 – Bevidstgøre brugere	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Er der en minimal erkendelse fra staten, den private sektor eller almindelige brugere af, at der er behov for at øge bevidstheden om cybersikkerhed og privatlivets fred?	1	Har I afgrænset en specifik målgruppe for brugeroplysning, f.eks. brugere i al almindelighed, unge, erhvervsbrugere (som kan opdeles yderligere: SMV'er, OES, distributionssystemoperatører osv.)?	1	Har I udarbejdet kommunikationsplaner/strategier for kampagnerne?	1	Udarbejder I parametre for evaluering af kampagnen i planlægningsfasen?	1	Har I indført mekanismer til at sikre, at oplysningskampagner hele tiden er relevante i forhold til teknologiske fremskridt, ændringer i trusselsbilledet, retlige bestemmelser og nationale sikkerhedsdirektiver?	1
	2	Gennemfører offentlige agenturer lejlighedsvise kampagner om cybersikkerhed inden for deres organisation, f.eks. i kølvandet på en cybersikkerhedshændelse?	0	Udarbejder I en projektplan for at øge kendskabet til informationssikkerhed og beskyttelse af privatlivets fred?	1	Har I en procedure for at skabe indhold på statsligt niveau?	1	Evaluerer I kampagnerne efter gennemførelsen?	1	Foretager I periodiske evalueringer eller undersøgelser for at måle holdningsændringer eller adfærdsændringer i forhold til cybersikkerhed og beskyttelse af privatlivets fred på tværs af den private og offentlige sektor?	1

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
5 – Bevidstgøre brugere	3	Gennemfører offentlige agenturer lejlighedsvise oplysningskampagner om cybersikkerhed over for den brede offentlighed? *F.eks.* i kølvandet på en cybersikkerhedshændelse.	0	Råder I over tilgængelige og let identificerbare ressourcer (f.eks. en fælles onlineportal, oplysningsværktøjer) til alle de brugere, der ønsker at få mere at vide om cybersikkerhed og beskyttelse af privatlivets fred?	1	Har I nogen mekanismer til at identificere målområder for bevidstgørelse (dvs. ENISA's trusselslandskab, nationale landskaber, internationale landskaber, feedback fra nationale cyberkriminalitetscentre osv.)?	1	Har I indført mekanismer til at identificere de mest relevante medier eller kommunikationskanaler afhængigt af målgruppen for at maksimere udbredelsen og engagementet, *f.eks.* forskellige typer digitale medier, brochurer, e-mails, undervisningsmateriale, plakater på områder med mange mennesker, tv, radio osv.?	1	Rådfører I jer med adfærdseksperter for at tilpasse kampagnen til målgruppen?	1
	4	-		-		Samler I interessenter, eksperter og kommunikationshold for at skabe indhold?	1			-	
	5	-		-		Inddrager og samarbejder I med den private sektor i jeres oplysningsarbejde for at fremme og udbrede budskaberne til et bredere publikum?	1	-		-	
	6	-		-		Udarbejder I specifikke oplysningstiltag for ledere i den offentlige, private eller akademiske sektor eller civilsamfundssektoren?	1	-		-	
	7	-		-		Deltager I i ENISA's kampagner i den europæiske måned for cybersikkerhed?	0	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
6 – Tilrettelægge cybersikkerhedsøvelser	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						

6 – Tilrettelægge cybersikkerhedsøvelser	1	Gennemfører I kriseøvelser i andre sektorer (ud over cybersikkerhed) på nationalt eller paneuropæisk plan?	1	Har I et program for cybersikkerhedsøvelser på nationalt plan?	1	Involverer I alle relaterede myndigheder i den offentlige forvaltning? (selv hvis scenariet er sektorspecifikt)	1	Skriver I efter handlingsrapporter/evalueringsrapporter?	1	Har I analysekapacitet for indhøstede erfaringer vedrørende cybersikkerhed (rapporteringsprocedurer, analyse, afhjælpning)?	1
	2	Er der afsat ressourcer til udformning og planlægning af krisestyringsøvelser?	1	Gennemfører eller prioriterer I øvelser i cyberkrisestyring vedrørende vitale samfundsmæssige funktioner og kritisk infrastruktur?	1	Inddrager I den private sektor i planlægningen og gennemførelsen af øvelserne?	1	Afprøver I planer og procedurer på nationalt plan?	1	Har I en fastlagt procedure for indhøstede erfaringer?	1
	3	-		Har I udpeget et koordineringsorgan, der skal føre tilsyn med udformningen og planlægningen af cybersikkerhedsøvelser (offentligt agentur, konsulentvirksomhed ...)?	0	Organiserer I sektorspecifikke øvelser på nationalt og/eller internationalt plan?	1	Deltager I i cybersikkerhedsøvelser på paneuropæisk plan?	1	Tilpasser I øvelsesscenarierne afhængigt af den seneste udvikling (teknologiske fremskridt, globale konflikter, trusselsbillede ...)?	1
	4	-		-		Organiserer I øvelser på tværs af alle de kritiske sektorer, der er nævnt i bilag II til NIS-direktivet?	1	-		Justerer I jeres krisestyringsprocedurer med andre medlemsstater for at sikre en effektiv fælleseuropæisk krisestyring?	1
	5	-		-		Organiserer I cybersikkerhedsøvelser mellem og/eller på tværs af sektorer?	1	-		Har I en mekanisme til hurtigt at tilpasse strategien, planerne og procedurerne på grundlag af erfaringerne fra øvelserne?	0
	6	-		-		Organiserer I cybersikkerhedsøvelser, der er specifikke for forskellige niveauer (teknisk og operationelt niveau, procedureniveau, beslutningsniveau, politisk niveau osv.)?	0	-		-	

NCSS-mål	#	Level 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
7 – Styrke uddannelses- og undervisningsprogrammer	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Overvejer I at udvikle uddannelsesprogrammer inden for cybersikkerhed?	1	Har I kurser, der er dedikeret til cybersikkerhed?	1	Indgår cybersikkerhedskultur i jeres land i den tidlige fase af de studerendes uddannelsesforløb? Prioriterer I f.eks. cybersikkerhed på mellemskole- og gymnasieniveau?	1	Opfordrer I til, at medarbejdere i den private og offentlige sektor bliver akkrediteret eller certificeret?	1	Har I indført mekanismer til at sikre, at uddannelsesprogrammer hele tiden er relevante i forhold til nuværende og nye teknologiske fremskridt, ændringer i trusselsbilledet, retlige bestemmelser og nationale sikkerhedsdirektiver?	1
	2	-		Tilbyder universiteter i jeres land ph.d.-forløb inden for cybersikkerhed som en uafhængig disciplin og ikke som datalogi?	1	Har I nationale forskningslaboratorier og uddannelsesinstitutioner, som er specialiseret i cybersikkerhed?	1	Har jeres land udarbejdet uddannelses- eller mentorprogrammer inden for cybersikkerhed for at støtte nationale nystartede virksomheder og SMV'er?	1	Opretter I akademiske ekspertisecentre inden for cybersikkerhed, der skal fungere som knudepunkter for forskning og uddannelse?	1
	3	-		Har I planer om at uddanne undervisere, uanset deres fagområde, i spørgsmål vedrørende informationssikkerhed og privatlivets fred, *f.eks.* onlinesikkerhed, beskyttelse af personoplysninger og cybermobning?	1	Tilskynder/finansierer I særlige cybersikkerhedskurser og uddannelsesplaner for ansatte i medlemsstaternes arbejdsformidlinger?	1	Støtter I aktivt indarbejdelse af kurser om informationssikkerhed på højere læreanstalter, ikke kun for datalogistuderende, men også for andre fagområder, *f.eks.* kurser, der er skræddersyet til erhvervets behov?	1	Deltager akademiske institutioner i ledende drøftelser inden for uddannelse og forskning i cybersikkerhed på internationalt plan?	0
	4	-		-		Har I kurser i cybersikkerhed og/eller et specialiseret pensum for EQF (den europæiske referenceramme for kvalifikationer) på niveau 5-8?	1	Vurderer I regelmæssigt kvalifikationskløften (mangel på medarbejdere inden for cybersikkerhed) inden for informationssikkerhed?	1	-	
	5	-		-		Tilskynder og/eller støtter I initiativer til at indarbejde kurser i internetsikkerhed i grundskolen og på ungdomsuddannelser?	1	Fremmer I netværkssamarbejde og informationsudveksling mellem akademiske institutioner på både nationalt og internationalt plan?	1		

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
7 - Styrke uddannelses- og undervisningsprogrammer	6	-		-		Finansierer I, eller tilbyder I gratis kurser i grundlæggende cybersikkerhed til borgerne?	0	Inddrager I på nogen måde den private sektor i uddannelsesinitiativer vedrørende cybersikkerhed, *f.eks.* udformning og gennemførelse af kurser, praktikophold, praktikforløb osv.?	1	-	
	7	-		-		Afholder I årlige informationssikkerhedsarrangementer (f.eks. hackingkonkurrencer eller hackathons)?	0	Benytter I finansieringsordninger for at fremme optaget på cybersikkerhedsuddannelser, f.eks. stipendier, garanterede lærlingepladser/praktikophold, garanteret beskæftigelse i bestemte brancher eller roller i den offentlige sektor?	0	-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
8 – Fremme FoU	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I gennemført undersøgelser eller analyser for at fastlægge prioriteter for FoU inden for cybersikkerhed?	1	Har I en procedure til at definere FoU-prioriteter (f.eks. nye emner inden for afskrækkelse, beskyttelse, opdagelse og tilpasning til nye former for cyberangreb)?	1	Er der planer om at forbinde FoU-initiativer med realøkonomien?	1	Er FoU-initiativer inden for cybersikkerhed i overensstemmelse med relevante strategiske mål, f.eks. det digitale indre marked, Horisont 2020, det digitale Europa og EU's strategi for cybersikkerhed?	1	Viderefører I på nationalt plan samarbejdet med eventuelle internationale FoU-initiativer vedrørende cybersikkerhed?	1
	2	-		Er den private sektor involveret i fastsættelsen af FoU-prioriteter?	1	Er der iværksæt nationale projekter vedrørende cybersikkerhed?	1	Findes der en evalueringsordning for FoU-initiativer?	1	Er FoU-prioriteterne tilpasset den nuværende eller kommende lovgivning (på nationalt plan)?	1

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
8 – Fremme FoU	3	-		Er den akademiske verden involveret i fastsættelsen af FoU-prioriteter?	1	Har I lokale/regionale startup-økosystemer og andre netværkskanaler (f.eks. teknologiparker, innovationsklynger, netværksarrangementer/-platforme) for at fremme innovation (herunder nystartede cybersikkerhedsvirksomheder)?	1	Er der indgået samarbejdsaftaler med universiteter og andre forskningsfaciliteter?	1	Deltager I i førende drøftelser om et eller flere af de seneste FoU-emner på internationalt plan?	0
	4	-		Findes der nationale FoU-initiativer vedrørende cybersikkerhed?	0	Investeres der i FoU-programmer inden for cybersikkerhed i den akademiske verden og i den private sektor?	1	Findes der et anerkendt institutionelt organ, der fører tilsyn med FoU-aktiviteter inden for cybersikkerhed?	0	-	
	5	-		-		Har I professorater inden for industriel forskning på universiteter for at sikre sammenhæng mellem forskningsemner og markedsbehov?	1	-		-	
	6	-		-		Har I FoU-finansieringsprogrammer, der er specifikt målrettet cybersikkerhed?	0	-		-	

NCSS-mål	#	Level 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
9 – Give incitamenter til den private sektor til at investere i sikkerhedsforanstaltninger	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						

	1	Findes der en industripolitik, eller er der politisk vilje til at fremme udviklingen af cybersikkerhedsindustrien?	1	Er den private sektor involveret i udformningen af incitamenter?	1	Findes der økonomiske/lovgivningsmæssige eller andre typer incitamenter til at styrke investeringer i cybersikkerhed?	1	Er der nogen private aktører, der reagerer på incitamenter ved at investere i sikkerhedsforanstaltninger, *f.eks.* investorer med speciale i cybersikkerhed og ikke-specialiserede investorer?	1	Bliver incitamenter målrettet cybersikkerhedsspørgsmål i henhold til den seneste trusselsudvikling?	1

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
9 – Give incitamenter til den private sektor til at investere i sikkerhedsforanstaltninger	2	-		Har I udpeget specifikke cybersikkerhedsemner, der skal udvikles, f.eks. kryptografi, privatlivets fred, ny form for autentifikation, kunstig intelligens til cybersikkerhed...?	0	Yder I støtte (f.eks. skatteincitamenter) til nystartede cybersikkerhedsvirksomheder og SMV'er?	1	Giver I den private sektor incitamenter til at fokusere på sikkerheden ved banebrydende teknologier, *f.eks.* 5G, kunstig intelligens, tingenes internet, kvantedatabehandling ...?	1	-	
	3	-		-		Giver I investorer fra den private sektor skatteincitamenter eller anden økonomisk motivation til at investere i nystartede cybersikkerhedsvirksomheder?	1	-		-	
	4	-		-		Letter I adgangen for nystartede cybersikkerhedsvirksomheder og SMV'er i forbindelse med offentlige udbud?	0	-		-	
	5	-		-		Er der midler til rådighed til incitamenter for den private sektor?	0	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
10 – Forbedre cybersikkerheden i forsyningskæden	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						

	1	Har I gennemført en undersøgelse om god sikkerhedspraksis vedrørende administrationen af den forsyningskæde, der benyttes i forbindelse med indkøb i forskellige industrisegmenter og/eller i den offentlige sektor?	1	Udfører I cybersikkerhedsvurderinger i hele forsyningskæden for IKT-tjenester og -produkter i kritiske sektorer (som anført i bilag II til direktivet om net- og informationssikkerhed (2016/1148))?	1	Benytter I en sikkerhedscertificeringsordning for IKT-baserede produkter og tjenester, f.eks. SOG-IS MRA i Europa (gruppen af højtstående embedsmænd for informationssystemers sikkerhed, aftale om gensidig anerkendelse), aftalen om anerkendelse af de fælles kriterier, nationale initiativer, sektorspecifikke initiativer...?	1	Har I indført en procedure for ajourføring af cybersikkerhedsvurderingerne af forsyningskæden for IKT-tjenester og -produkter i kritiske sektorer (som anført i bilag II til NIS-direktivet (2016/1148))?	1	Har I detektionssonder i centrale elementer i forsyningskæden for at opdage tidlige tegn på sikkerhedsbrud, f.eks. sikkerhedskontrol på ISP-niveau, sikkerhedssonder i vigtige infrastrukturkomponenter osv.?	1

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
10 – Forbedre cybersikkerheden i forsyningskæden	2	-		Er der i offentlige myndigheders indkøbspolitikker indført standarder for at sikre, at udbydere af IKT-produkter eller -tjenester opfylder grundlæggende informationssikkerhedskrav, f.eks. ISO/IEC 27001 og 27002, ISO/IEC 27036...?	1	Fremmer I aktivt sikkerhed og privatlivets fred ved at udforme bedste praksis inden for udvikling af IKT-produkter og -tjenester, f.eks. proces for udvikling af sikker software, proces for tingenes internet?	1	Har I indført en procedure for identifikation af cybersikkerhedsmæssige svage led i forsyningskæden til kritiske sektorer (som anført i bilag II til NIS-direktivet (2016/1148))?	1	-	
	3	-		-		Udvikler og tilbyder I et centraliseret katalog med uddybende oplysninger om eksisterende standarder for informationssikkerhed og beskyttelse af privatlivets fred, som kan tilpasses og anvendes af SMV'er?	1	Har I indført mekanismer til at sikre, at IKT-produkter og -tjenester, der er kritiske for operatører af væsentlige tjenester, er cyberrobuste (*dvs.* at de er i stand til at opretholde tilgængelighed og sikkerhed i tilfælde af en cyberhændelse), *f.eks.* gennem afprøvning, regelmæssige vurderinger, opdagelse af kompromitterede elementer osv.?	1	-	
	4	-				Deltager I aktivt i udformningen af en EU-certificeringsramme for digitale IKT-produkter, -tjenester og -processer som fastsat i EU's cybersikkerhedsforordning (forordning (EU) 2019/881), f.eks. deltagelse i den europæiske cybersikkerhedscertificeringsgruppe, fremme af tekniske standarder og procedurer for sikkerhed af IKT-produkter/-tjenester?	0	Fremmer I udviklingen af certificeringsordninger, der er rettet mod SMV'er, for at styrke indførslen af standarder for informationssikkerhed og beskyttelse af privatlivets fred?	0	-	
	5	-		-		Giver I nogen form for incitamenter til SMV'er for at indføre standarder for sikkerhed og beskyttelse af privatlivets fred?	0	Har I nogen bestemmelser, der kan tilskynde store virksomheder til at øge cybersikkerheden for små virksomheder i deres forsyningskæder, *f.eks.* cybersikkerhedsknudepunkt, uddannelses- og oplysningskampagner...?	0	-	

	6	-		-		Tilskynder I softwareleverandører til at støtte SMV'er ved at garantere sikre standardkonfigurationer i produkter, der er målrettet små organisationer?	0	-		-		

4.1.3 Gruppe nr. 3: jura og offentlige udbud

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
11 – Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Er der generel enighed om, at CII-operatører bidrager til den nationale sikkerhed?	1	Har I en metode til at identificere væsentlige tjenester?	1	Har I gennemført NIS-direktivet (2016/1148)?	1	Har I en procedure for ajourføring af risikoregistret?	1	Udarbejder og ajourfører I rapporter om trusselslandskabet?	1

2	-		Har I en metode til indkredsning af CII'er?	1	Har I gennemført direktivet om europæisk kritisk infrastruktur (2008/114) om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre?	1	Har I andre mekanismer til at måle, om de tekniske og organisatoriske foranstaltninger, som OES'ere har gennemført, er hensigtsmæssige i forhold til at styre sikkerhedsrisiciene i net- og informationssystemer, f.eks. regelmæssige cybersikkerhedsrevisioner, nationale rammer for gennemførelse af standardforanstaltninger, tekniske værktøjer, der stilles til rådighed af staten, såsom detektionssonder eller systemspecifik konfigurationsrevision...?	1	Kan I, afhængigt af den seneste udvikling i trusselslandskabet, medtage en ny sektor i jeres handlingsplan for kritisk informationsinfrastruktur?	1
3	-		Har I en metode til at identificere en OES?	1	Har I et nationalt register over identificerede OES'er opdelt efter kritisk sektor?	1	Reviderer og ajourfører I regelmæssigt, mindst hvert andet år, listen over identificerede OES'er?	1	Kan I, afhængigt af den seneste udvikling i trusselslandskabet, indarbejde nye krav i jeres handlingsplan for kritisk informationsinfrastruktur?	1

NCSS-mål	#										
11 – Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester	4	-		Har I en metode til at identificere udbydere af digitale tjenester?	1	Har I et nationalt register over identificerede udbydere af digitale tjenester?	1	Har I andre mekanismer til at måle, om de tekniske og organisatoriske foranstaltninger, som udbydere af digitale tjenester har gennemført, er hensigtsmæssige i forhold til at styre sikkerhedsrisiciene i net- og informationssystemer, f.eks. regelmæssige cybersikkerhedsrevisioner, nationale rammer for gennemførelse af standardforanstaltninger, tekniske værktøjer, der stilles til rådighed af staten, såsom detektionssonder eller systemspecifik konfigurationsrevision...?	1	-	
	5	-		Er der en eller flere nationale myndigheder, der fører tilsyn med beskyttelsen af kritisk informationsinfrastruktur samt net- og informationssystemers sikkerhed, f.eks. som krævet i henhold til direktivet om net- og informationssikkerhed (2016/1148)?	1	Har I et nationalt risikoregister over identificerede eller kendte risici?	1	Reviderer og ajourfører I regelmæssigt, mindst hvert andet år, listen over identificerede udbydere af digitale tjenester?	1	-	
	6	-		Udvikler I sektorspecifikke beskyttelsesplaner, der f.eks. omfatter grundlæggende cybersikkerhedsforanstaltninger (obligatoriske eller vejledende)?	0	Har I en metode til at kortlægge afhængigheder i CII?	1	Benytter I en sikkerhedscertificeringsordning (national eller international) til at hjælpe OET og udbydere af digitale tjenester med at identificere sikre IKT-produkter, f.eks. SOG-IS MRA i Europa, nationale initiativer?	1	-	
	7	-		-		Anvender I metoder til risikostyring til at identificere, kvantificere og styre risici, der er relateret til CII'er på nationalt plan?	1	Benytter I en sikkerhedscertificeringsordning eller kvalifikationsprocedure til at vurdere tjenesteudbydere, der arbejder med OET'er, f.eks. tjenesteudbydere inden for opdagelse af hændelser, beredskab, cybersikkerhedsrevision, cloudtjenester, smart cards...?	1	-	

	8	-		-		Deltager I i en høringsproces for at identificere grænseoverskridende afhængighed?	1	Har I indført mekanismer til måling af OES og udbydere af digitale tjenesters overholdelse af grundlæggende cybersikkerhedsforanstaltninger?	0	-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
11 – Beskytte kritisk informationsinfrastruktur, OES og udbydere af digitale tjenester	9					Har I et centralt kontaktpunkt med ansvar for koordinering af spørgsmål vedrørende sikkerheden i net- og informationssystemer på nationalt plan og grænseoverskridende samarbejde på EU-plan?	1	Har I indført foranstaltninger til at sikre kontinuiteten i de tjenester, der leveres af kritiske informationsinfrastrukturer, f.eks. foregribelse af kriser, procedurer for genopbygning af kritiske informationssystemer, forretningskontinuitet uden IT, backup-procedurer for luftgab...?	0		
	10					Definerer I grundlæggende cybersikkerhedsforanstaltninger (obligatoriske eller vejledende) for udbydere af digitale tjenester og alle sektorer, der er anført i bilag II til direktivet om net- og informationssikkerhed (2016/1148)?	1				
	11	-		-		Stiller I værktøjer eller metoder til rådighed for at opdage cyberhændelser?	1	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
12 – Bekæmpe cyberkriminalitet	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I gennemført en undersøgelse for at identificere kravene til retshåndhævelse (retsgrundlag, ressourcer, færdigheder osv.) for effektivt at bekæmpe cyberkriminalitet?	1	Er jeres nationale retlige ramme i fuld overensstemmelse med den relevante EU-lovgivning, herunder direktiv 2013/40/EU om angreb på informationssystemer, f.eks. ulovlig adgang til informationssystemer, ulovligt indgreb i systemet, ulovligt indgreb i data, ulovlig opfangning, redskaber, der anvendes til at begå lovovertrædelser...?	1	Har anklagemyndigheden enheder, der er dedikeret til at håndtere cyberkriminalitet?	1	Indsamler I statistikker i henhold til bestemmelserne i artikel 14, stk. 1, i direktiv 2013/40/EU (direktivet om angreb på informationssystemer)?	1	Har I interinstitutionelle uddannelsesworkshopper for retshåndhævende myndigheder, dommere, anklagere og nationale/statslige CSIRT'er på nationalt plan og/eller på multilateralt plan?	1
	2	Har I gennemført en undersøgelse for at identificere kravene til anklagere og dommere (retsgrundlag, ressourcer, færdigheder...) med henblik på effektivt at bekæmpe cyberkriminalitet?	1	Er der nogen lovbestemmelser om identitetstyveri på nettet og tyveri af personoplysninger?	1	Har I et øremærket budget til enheder til bekæmpelse af cyberkriminalitet?	1	Indsamler I særskilte statistikker om cyberkriminalitet, f.eks. operationelle statistikker, statistikker over tendenser inden for cyberkriminalitet, statistikker over indtægter fra cyberkriminalitet og forvoldte skader...?	1	Deltager I i koordinerede tiltag på internationalt plan for at afskære kriminelle aktiviteter, f.eks. infiltration af fora for kriminel hacking, organiserede cyberkriminelle grupper, fjernelse af markeder på det mørke internet og botnets...?	1
	3	Har jeres land undertegnet Europarådets Budapestkonvention om it-kriminalitet?	1	Er der lovbestemmelser om krænkelse af intellektuel ejendom og ophavsrettigheder på internettet?	1	Har I oprettet et centralt organ/en central enhed til at koordinere aktiviteterne inden for bekæmpelse af cyberkriminalitet?	1	Evaluerer I, om uddannelsen af retshåndhævende myndigheder, medarbejdere i retsvæsenet og nationale CSIRT'er er tilstrækkelig til at bekæmpe cyberkriminalitet?	1	Er der en klar adskillelse af opgaver på tværs af CSIRT'er, retshåndhævende myndigheder og retsvæsenet (anklagere og dommere), når de samarbejder om at håndtere cyberkriminalitet?	1

	4			Er der lovbestemmelser om bekæmpelse af chikane på internettet og internetmobning?	1	Har I etableret samarbejdsmekanismer mellem relevante nationale institutioner, der er involveret i bekæmpelse af cyberkriminalitet, herunder retshåndhævende nationale CSIRT'er?	1	Foretager I regelmæssige evalueringer for at sikre, at der er afsat tilstrækkelige ressourcer (menneskelige ressourcer, budget og værktøjer) til enheder inden for de retshåndhævende myndigheder til bekæmpelse af cyberkriminalitet?	1	Fremmer lovgivningen samarbejdet mellem CSIRT'er/retshåndhævende myndigheder og retsvæsenet (anklagere og dommere)?	1
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
12 – Bekæmpe cyberkriminalitet	5			Er der nogen lovbestemmelser om computerrelateret svig, f.eks. overholdelse af bestemmelserne i Europarådets Budapestkonvention om it-kriminalitet	1	Samarbejder og udveksler I oplysninger med andre medlemsstater om bekæmpelse af cyberkriminalitet?	1	Foretager I regelmæssige evalueringer for at sikre, at der er afsat tilstrækkelige ressourcer (menneskelige ressourcer, budget og værktøjer) til enheder inden for retsforfølgende myndigheder til bekæmpelse af cyberkriminalitet?	1	Deltager I i opbygningen og vedligeholdelsen af standardiserede værktøjer og metoder, formularer og procedurer, der skal deles med EU-interessenter (retshåndhævende myndigheder, CSIRT'er, ENISA, Europols EC3 ...)?	1
	6	-		Er der nogen lovbestemmelser om beskyttelse af børn på nettet, f.eks. overholdelse af bestemmelserne i direktiv 2011/93/EU og Europarådets Budapestkonvention om it-kriminalitet?	1	Samarbejder og udveksler I oplysninger med EU-agenturer (f.eks. Europols EC3, Eurojust, ENISA) om bekæmpelse af cyberkriminalitet?	1	Har I afdelinger med særlige domstole eller specialiserede dommere til at behandle sager om cyberkriminalitet?	1	Har I indført avancerede mekanismer til at afskrække enkeltpersoner fra at blive tiltrukket af eller involveret i cyberkriminalitet?	0
	7	-		Har I udpeget et operationelt nationalt kontaktpunkt til at udveksle oplysninger og besvare hasteanmodninger om oplysninger fra andre medlemsstater vedrørende lovovertrædelser i henhold til direktiv 2013/40/EU (direktivet om angreb på informationssystemer)?	1	Har I de rette værktøjer til at bekæmpe cyberkriminalitet, f.eks. taksonomi og klassificering af cyberkriminalitet, værktøjer til indsamling af elektronisk bevismateriale, computerkriminaltekniske værktøjer, platforme for pålidelig deling...?	1	Er der nogen bestemmelser om at yde støtte og bistand til ofre for cyberkriminalitet (almindelige brugere, SMV'er, store virksomheder)?	1	Anvender jeres land EU's plan og/eller beredskabsprotokollen om retshåndhævelsesindsats (EU LE ERP) til effektivt at reagere på omfattende cyberhændelser?	0
	8			Er der en dedikeret cyberkriminalitetsenhed i jeres retshåndhævende myndighed?	1	Har I standardprocedurer for håndtering af elektronisk bevismateriale?	1	Har I oprettet en interinstitutionel ramme og samarbejdsmekanismer mellem alle relevante interessenter (f.eks. retshåndhævende myndigheder, nationale CSIRT'er, retsvæsen), herunder, hvor det er relevant, den private sektor (f.eks. operatører af væsentlige tjenester, tjenesteudbydere) for at reagere på cyberangreb?	1	-	

	9			Har I, jf. artikel 35 i Budapestkonventionen, udpeget et 24/7-kontaktpunkt?	1	Deltager jeres land i uddannelsesmuligheder, der tilbydes og/eller støttes af EU-agenturer (f.eks. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Fremmer lovgivningen samarbejdet mellem CSIRT'er og retshåndhævende myndigheder?	1	-	
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
12 – Bekæmpe cyberkriminalitet	10	-		Har I udpeget et operationelt nationalt 24/7-kontaktpunkt for EU's beredskabsprotokol vedrørende retshåndhævelse (EU LE ERP) til at reagere på større cyberangreb?	1	Overvejer jeres land at vedtage den 2. tillægsprotokol til Europarådets Budapestkonvention om it-kriminalitet?	0	Har I indført mekanismer (f.eks. værktøjer og procedurer) til at lette informationsudvekslingen og samarbejdet mellem CSIRT/retshåndhævende myndigheder samt eventuelt retsvæsenet (anklagere og dommere) inden for bekæmpelse af cyberkriminalitet?	1	-	
	11			Tilbyder I regelmæssigt specialiseret uddannelse til interessenter, der er involveret i bekæmpelse af cyberkriminalitet (retshåndhævende myndigheder, retsvæsen, CSIRT'er), f.eks. uddannelseskurser om indberetning/retsforfølgning af cyberrelaterede forbrydelser, uddannelse i indsamling af elektronisk bevismateriale og sikring af integritet i hele den digitale opbevaringskæde og computerkriminalteknik?	1						
	12			Har jeres land ratificeret/tiltrådt Europarådets Budapestkonvention om it-kriminalitet?	1			-	-	-	
	13	-		Har jeres land undertegnet og ratificeret tillægsprotokollen (kriminalisering af handlinger af racistisk og fremmedfjendsk karakter begået ved hjælp af computersystemer) til Europarådets Budapestkonvention om it-kriminalitet?	0	-	-	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
13 – Indføre mekanismer til indberetning af hændelser	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I uformelle informationsudvekslingsmekanismer om cybersikkerhedshændelser mellem private organisationer og nationale myndigheder?	1	Har I en ordning for indberetning af hændelser for de sektorer, der er nævnt i bilag II til NIS-direktivet?	1	Har I en obligatorisk ordning for indberetning af hændelser, der fungerer i praksis?	1	Har I en harmoniseret procedure for sektorspecifikke ordninger for indberetning af hændelser?	1	Udarbejder I årlige hændelsesrapporter?	1
	2	-		Har I gennemført kravene til underretning for udbydere af telekommunikationstjenester i overensstemmelse med artikel 40 i direktivet (EU 2018/1972)? I henhold til direktivet skal medlemsstaterne sikre, at udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester uden unødig forsinkelse underretter den kompetente myndighed om en sikkerhedshændelse, der har haft en betydelig indvirkning på driften af net eller tjenester.	1	Findes der en koordinerings-/samarbejdsmekanisme for forpligtelser om indberetning af hændelser vedrørende GDPR, NIS-direktivet, artikel 40 (tidl. artikel 13a) og eIDAS?	1	Har I en ordning for indberetning af hændelser for andre sektorer end dem, der er nævnt i NIS-direktivet?	1	Findes der rapporter om cybersikkerhedslandskabet eller andre former for analyser udarbejdet af den enhed, der modtager hændelsesrapporterne?	1

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
13 – Indføre mekanismer til indberetning af hændelser	3	-		Har I gennemført kravene til underretning for udbydere af tillidstjenester i overensstemmelse med artikel 19 i eIDAS-forordningen (forordning (EU) nr. 910/2014)? I henhold til artikel 19 skal udbydere af tillidstjenester bl.a. underrette tilsynsorganet om væsentlige hændelser/brud.	1	Har I passende værktøjer til at sikre fortroligheden og integriteten af de oplysninger, der udveksles via de forskellige indberetningskanaler?	1	Måles effektiviteten af procedurerne for indberetning af hændelser, f.eks. indikatorer for hændelser, der er blevet indberettet via de relevante kanaler, tidsplan for hændelsesindberetningen...?	1	-	
	4	-		Har I gennemført kravene til underretning for udbydere af digitale tjenester i overensstemmelse med artikel 16 i NIS-direktivet? I henhold til artikel 16 skal udbydere af digitale tjenester uden unødig forsinkelse underrette den kompetente myndighed eller den nationale CSIRT om enhver hændelse, der har en væsentlig indvirkning på leveringen af en tjeneste som omhandlet i bilag III, som de udbyder i Unionen.	1	Har I en platform/et værktøj til at lette underretningsprocessen?	0	Har I en fælles taksonomi på nationalt plan for klassificering af hændelser og kategorier af tilgrundliggende årsager?	0	-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
14 – Styrke privatlivets fred og databeskyttelse	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Har I gennemført undersøgelser eller analyser for at identificere områder, hvor der kan ske forbedringer for bedre at beskytte borgernes ret til privatlivets fred?	1	Er den nationale databeskyttelsesmyndighed involveret i cybersikkerhedsrelaterede områder (f.eks. udarbejdelse af nye love og bestemmelser om cybersikkerhed, fastlæggelse af minimumssikkerhedsforanstaltninger)?	1	Fremmer I bedste praksis for sikkerhedsforanstaltninger og indbygget databeskyttelse for den offentlige og/eller private sektor?	1	Foretager I regelmæssige evalueringer for at sikre, at der er afsat tilstrækkelige ressourcer (menneskelige ressourcer, budget og værktøjer) til databeskyttelsesmyndigheden?	1	Har I indført mekanismer til overvågning af den seneste teknologiske udvikling med henblik på at tilpasse relevante retningslinjer og retlige bestemmelser/forpligtelser?	1
	2	Har I udarbejdet et retsgrundlag på nationalt plan for at håndhæve den generelle forordning om databeskyttelse (forordning (EU) 2016/679), f.eks. fastholdelse eller indførelse af mere specifikke bestemmelser eller begrænsninger af forordningens regler?	0	-		Lancerer I bevidstgørelses- og uddannelsesprogrammer om dette emne?	1	Opfordrer I organisationer og virksomheder til at blive certificeret i henhold til ISO/IEC 27701: 2019 om sikkerhedsteknikker udvidet til at omfatte privatlivsbeskyttelse?	1	Deltager/fremmer I aktivt FoU-initiativer vedrørende teknologier til beskyttelse af privatlivet (PET)?	0
	3	-		-		Koordinerer I procedurerne for indberetning af hændelser med databeskyttelsesmyndigheden?	1	-		-	
	4	-		-		Fremmer og støtter I udviklingen af tekniske standarder for informationssikkerhed og privatlivets fred? Er de specifikt tilpasset små og mellemstore virksomheder (SMV'er)?	0	-		-	

	5	-		-		Tilbyder I praktiske og skalerbare retningslinjer til støtte for forskellige typer dataansvarlige om overholdelse af lovkrav og forpligtelser vedrørende beskyttelse af privatlivets fred og databeskyttelse?	0	-		-	

4.1.4 Gruppe nr. 4: Samarbejde

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
15 – Etablering af et offentligt-privat partnerskab (OPP'er)	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						
	1	Er det den almindelige opfattelse, at OPP'er på forskellige måder bidrager til at øge cybersikkerhedsniveauet i landet, f.eks. udveksling af interesse i udbredelsen af cybersikkerhedsindustrien, samarbejde om udarbejdelse af en relevant lovramme for cybersikkerhed, styrkelse af FoU...?	1	Har I en national handlingsplan for oprettelse af OPP'er?	1	Har I oprettet nationale offentlig-private partnerskaber?	1	Har I oprettet offentlig-private partnerskaber på tværs af sektorer?	1	Kan I tilpasse eller oprette OPP'er afhængigt af den seneste teknologiske og lovgivningsmæssige udvikling?	1
	2	-		Fastsætter I et retsgrundlag eller et kontraktligt grundlag (specifik lovgivning, NDA'er, intellektuel ejendomsret), der omfatter OPP'er?	1	Har I oprettet sektorspecifikke offentlig-private partnerskaber?	1	Er fokus i de oprettede OPP'er også på samarbejde mellem offentlige organer og mellem offentlige og private enheder?	1		
	3	-		-		Tilbyder I finansiering til oprettelse af OPP'er?	1	Fremmer I OPP'er blandt små og mellemstore virksomheder (SMV'er)?	1	-	
	4	-		-		Står offentlige institutioner generelt i spidsen for OPP'erne, dvs. et centralt kontaktpunkt fra den offentlige sektor, der styrer og koordinerer OPP'et, er offentlige organer på forhånd enige om, hvad de ønsker at opnå, er der klare retningslinjer fra de offentlige myndigheder om deres behov og begrænsninger for den private sektor...?	1	Måles resultaterne af OPP'er?	1	-	

	5	-		-		Er I medlem af det kontraktlige offentligt-private partnerskab med Den Europæiske Cybersikkerhedsorganisation (ECSO)?	0	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
15 – Etablere et offentligt-privat partnerskab (OPP'er)	6	-		-		Har I et eller flere OPP'er, der arbejder med CSIRT-aktiviteter?	0	-		-	
	7					Har I et eller flere OPP'er, der beskæftiger sig med spørgsmål vedrørende beskyttelse af kritisk informationsinfrastruktur?	0				
	8	-		-		Har I et eller flere OPP'er, der arbejder på at øge bevidstheden om cybersikkerhed og udvikle kompetencer?	0	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
16 – Institutionalisere samarbejdet mellem offentlige organer	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		
	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0						

	1	Har I uformelle samarbejdskanaler mellem offentlige organer?	1	Findes der en national samarbejdsordning med fokus på cybersikkerhed, f.eks. rådgivende udvalg, styringsgrupper, fora, råd, cybercentre eller ekspertmøder?	1	Deltager de offentlige myndigheder i samarbejdsordningen?	1	Garanterer I, at der som minimum findes samarbejdskanaler for cybersikkerhed mellem følgende offentlige organer: efterretningstjenester, nationale retshåndhævende myndigheder, anklagemyndigheder, statslige aktører, nationale CSIRT'er og militæret?	1	Modtager offentlige agenturer ensartede minimumsoplysninger om den seneste udvikling i trusselslandskabet og situationsrapporter om cybersikkerhed?	1
	2	-		-		Har I oprettet samarbejdsplatforme til udveksling af oplysninger?	1	Måles de forskellige samarbejdsordningers succeser og begrænsninger i forhold til at fremme et effektivt samarbejde?	1	-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
16 – Institutionalisere samarbejdet mellem offentlige organer	3	-		-		Har I defineret samarbejdsplatformens anvendelsesområde (f.eks. opgaver og ansvarsområder, antal emneområder)?	1	-		-	
	4	-		-		Afholder I årlige møder?	1	-		-	
	5	-		-		Har I samarbejdsmekanismer mellem kompetente myndigheder på tværs af geografiske regioner, f.eks. netværk af sikkerhedskorrespondenter pr. region, cybersikkerhedsmedarbejder i regionale handelskamre?	1	-		-	

NCSS-mål	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
17 – Deltage i internationalt samarbejde (ikke kun med EU-medlemsstater)	(a)	Er målet dækket ind i den nuværende NCSS, eller planlægger I at dække det i næste udgave?	1	Findes der uformelle metoder eller aktiviteter, som bidrager til at nå målet på en ikke-koordineret måde?	1	Har I en formelt defineret og dokumenteret handlingsplan?	1	Gennemgår I handlingsplanen i forhold til målet om at teste resultaterne af den?	1	Har I indført mekanismer til at sikre, at handlingsplanen tilpasses udviklingen i miljøet på en dynamisk måde?	1
	(b)			Har I defineret de tilsigtede resultater, vejledende principper eller nøgleaktiviteter i handlingsplanen?	1	Har I en handlingsplan med en klar ressourceallokering og -styring?	1	Gennemgår I handlingsplanen i forhold til målet om at sikre, at den er korrekt prioriteret og optimeret?	1		

	(c)			Er handlingsplanen eventuelt gennemført og allerede effektiv i begrænset omfang?	0							
	1	Har I en strategi for internationalt engagement?	1	Har I samarbejdsaftaler med andre lande (bilaterale, multilaterale) eller partnere i andre lande, f.eks. informationsudveksling, kapacitetsopbygning, bistand?	1	Udveksler I oplysninger på strategisk niveau, f.eks. politik på højt niveau, risikoopfattelse osv.?	1	Deltager nationale offentlige cybersikkerhedsagenturer i jeres land i internationale samarbejdsordninger?	1	Fører I drøftelser om et eller flere emner inden for rammerne af multilaterale aftaler?	1
	2	Har I uformelle samarbejdskanaler med andre lande?	1	Har I et centralt kontaktpunkt, der kan varetage en forbindelsesfunktion for at sikre grænseoverskridende samarbejde med medlemsstaternes myndigheder (samarbejdsgruppe, CSIRT-netværk...)?	1	Udveksler I oplysninger på taktisk niveau, f.eks. efterretninger om trusselsaktører, ISAC, TTP'er?	1	Vurderer I regelmæssigt resultaterne af internationale samarbejdsinitiativer?	1	Fører I drøftelser om et eller flere emner inden for rammerne af internationale traktater eller konventioner?	1
NCSS-mål	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
17 – Deltage i internationalt samarbejde (ikke kun med EU-medlemsstater)	3	Har ledere i den offentlige sektor udtrykt intentioner om at deltage i internationalt samarbejde på cybersikkerhedsområdet?	1	Har I engagerede personer, der er involveret i internationalt samarbejde?	1	Udveksler I oplysninger på operationelt plan, f.eks. oplysninger om operationel koordinering, igangværende hændelser, IOC'er?	1	-		Fører I drøftelser eller forhandlinger om et eller flere emner i internationale ekspertgrupper, f.eks. den globale kommission for stabilitet i cyberspace (GCSC), ENISA-NIS-samarbejdsgruppen, FN's gruppe af regeringseksperter om informationssikkerhed (UNGGE)?	1
	4	-		-		Deltager I i internationale cybersikkerhedsøvelser?	1	-		-	
	5	-		-		Deltager I i internationale kapacitetsopbygningsinitiativer, f.eks. uddannelse, kompetenceudvikling, udarbejdelse af standardprocedurer?	0	-		-	
	6	-		-		Har I indgået aftaler om gensidig bistand med andre lande, *f.eks.* retshåndhævende myndigheders aktiviteter, retssager, gensidiggørelse af indsatskapaciteter for hændelser, deling af cybersikkerhedsaktiver?	0	-		-	

	7	-		-		Har I undertegnet eller ratificeret internationale traktater eller konventioner på cybersikkerhedsområdet, f.eks. den internationale adfærdskodeks for informationssikkerhed, konventionen om it-kriminalitet?	0	-		-	

4.2 RETNINGSLINJER FOR ANVENDELSE AF RAMMEN

Formålet med dette afsnit er at give medlemsstaterne nogle retningslinjer og anbefalinger til gennemførelsen af rammen og udfyldelsen af spørgeskemaet. Nedenstående anbefalinger stammer hovedsagelig fra den feedback, der er indsamlet fra interviewene med medlemsstaternes repræsentanter:

- **Forberede koordineringsaktiviteter med henblik på indsamling og konsolidering af data.** De fleste medlemsstater er enige om, at det bør tage ca. 15 manddage at foretage en sådan selvvurdering. For at kunne foretage selvvurderingen skal der rettes henvendelse til en lang række interessenter. Det anbefales derfor, at der afsættes tid til forberedelsesfasen for at identificere alle relevante interessenter i statslige organer, offentlige organer og den private sektor.
- **Identificere et centralt organ med ansvar for at gennemføre selvvurderingen på nationalt plan.** Eftersom der kan være mange interessenter involveret i indsamlingen af materiale for alle indikatorer i NCAF'en, anbefales det at udpege et centralt organ eller agentur, der får til opgave at gennemføre selvvurderingen ved at samarbejde og koordinere med alle relevante interessenter.
- **Bruge vurderingsøvelsen til at dele og kommunikere oplysninger om emner relateret til cybersikkerhed.** Medlemsstaternes erfaringer viste, at drøftelser (uanset om de er i form af individuelle interview eller kollektive workshopper) er en god lejlighed til at fremme dialog om cybersikkerhedsspørgsmål og udveksle fælles synspunkter og områder, hvor der kan ske forbedringer. Ud over at kaste lys over de vigtigste resultater kan deling af resultater også bidrage til at fremme cybersikkerhedsspørgsmål.
- **Bruge NCSS som ramme til at udvælge de mål, der er genstand for vurderingen.** De 17 mål, der udgør NCAF'en, er fastsat med udgangspunkt i de mål, der normalt indgår i medlemsstaternes NCSS. De mål, der indgår i NCSS'en, bør anvendes til at afgrænse vurderingen. NCSS'en bør dog ikke begrænse vurderingen. NCSS'en er naturligvis koncentreret om prioriteter, og derfor er visse områder bevidst udeladt fra den. Det betyder imidlertid ikke, at en given kapacitet ikke er til stede. I tilfælde hvor et specifikt mål udelades fra NCSS, men hvor landet har cybersikkerhedskapacitet relateret til dette mål, kan der f.eks. foretages en vurdering af dette mål.
- **Når NCSS'ens anvendelsesområde udvides, skal det sikres, at fortolkningen af scorer er i overensstemmelse med udviklingen i NCSS.** NCSS' livscyklus er en flerårig proces. Nogle medlemsstaters NCSS gennemføres med en køreplan på normalt 3-5-år med ændringer i anvendelsesområdet for to på hinanden følgende udgaver af NCSS. Der skal i det lys udvises særlig omhu ved fremlæggelsen af resultaterne af selvvurderingen mellem to versioner af NCSS: ændringer i anvendelsesområdet kan helt konkret påvirke den endelige modenhedsscore. Det anbefales at sammenligne scorerne for de strategiske måls fulde anvendelsesområde fra et år til et andet (dvs. samlet generel score).

Påmindelse om scoringsmekanismen – eksempel på dækningsgrad

Scoringsmekanismen omfatter to niveauer af scorer:
(i) en **samlet generel dækningsgrad** baseret på den fuldstændige liste over strategiske mål i selvvurderingsrammen og
(ii) **en samlet specifik dækningsgrad** baseret på de strategiske mål, som medlemsstaten har udvalgt (og som normalt svarer til de mål, der er fastsat i det pågældende lands NCSS).

Som følge af metoden (se afsnit 3.1 om scoringsmekanismen) vil den samlede specifikke dækningsgrad være lig med eller højere end den generelle dækningsgrad, da sidstnævnte kan omfatte mål, som medlemsstaten ikke dækker, hvorved den generelle dækningsgrad reduceres. Når en medlemsstat tilføjer et nyt mål, vil den samlede dækningsgrad stige (dvs. at der

medtages flere modenhedsindikatorer), hvorimod den samlede specifikke modenhed kan falde (hvis det nyligt tilføjede mål er i startfasen og dermed har et lavt modenhedsniveau).

- **I forbindelse med udfyldelsen af spørgeskemaet til selvvurderingen skal det bemærkes, at det primære mål er at støtte medlemsstaterne i kapacitetsopbygning inden for cybersikkerhed.** Ved udfyldelsen af selvvurderingen anbefales det derfor, at der vælges det mest alment accepterede svar, selv om det i visse situationer kan være vanskeligt at besvare spørgsmålet på en bestemt måde. Hvis svaret på et spørgsmål f.eks. er JA for et bestemt anvendelsesområde, men er NEJ på et andet område, bør medlemsstaterne være opmærksomme på, at et NEJ-svar kræver handling: enten en afhjælpningsplan eller en plan for forbedring på et bestemt område, der skal tages i betragtning i den fremtidige udvikling

5. NÆSTE TRIN

5.1 FREMTIDIGE FORBEDRINGER

Under interview med medlemsstaternes repræsentanter og i løbet af dokumentationsundersøgelsen blev der også udpeget følgende anbefalinger til forbedring af den nuværende ramme for vurdering af national kapacitet som potentiel fremtidig udvikling:

- **Udvikle scoringsmekanismen for at forbedre nøjagtigheden.** Der kan f.eks. indtastes en procentdel af dækningen i stedet for det binære JA/NEJ-svar for bedre at kunne tage højde for kompleksiteten ved at konsolidere kapaciteten på nationalt plan. Der blev i første omgang valgt en enkel tilgang med JA/NEJ-svar.
- **Indføre kvantitative parametre til at måle effektiviteten af medlemsstaternes NCSS'er.** Rammen for vurdering af national kapacitet fokuserer nemlig på evaluering af modenhedsniveauet af medlemsstaternes cybersikkerhedskapacitet. Dette kan suppleres med parametre til at måle effektiviteten af de aktiviteter og handlingsplaner, som medlemsstaterne gennemfører for at opbygge denne kapacitet. Det forekom ikke realistisk at udarbejde sådanne effektivitetsparametre i den nuværende fase, fordi der kun var lidt feedback fra området, det var vanskeligt at finde meningsfulde indikatorer, der forbinder output med gennemførelsen af NCSS, og der var vanskeligheder med at opbygge realistiske indikatorer, der efterfølgende kan indsamles. Dette er dog fortsat et emne for det fremtidige arbejde.
- **Skifte fra en selvvurderingsøvelse til en vurderingsmetode.** En mulig fremtidig udvikling af rammen kunne være at gå over til en vurderingsmetode med henblik på at vurdere modenheden af medlemsstaternes cybersikkerhedskapacitet på en mere ensartet måde. Hvis en tredjepart udfører vurderingen, kan det faktisk vise sig muligt at minimere eventuelle skævheder.

BILAG A – OVERSIGT OVER RESULTATERNE AF DOKUMENTATIONSUNDERSØGELSEN

Bilag A indeholder en sammenfatning af ENISA's tidligere arbejde med NCSS og en gennemgang af relevante offentligt tilgængelige modenhedsmodeller om cybersikkerhedskapacitet. Følgende antagelser blev taget i betragtning ved udvælgelsen og gennemgangen af modellerne:

- Ikke alle modeller er baseret på en stringent forskningsmetodologi
- Modellernes struktur og resultater forklares ikke altid grundigt med klare forbindelser mellem de forskellige elementer, der karakteriserer hver model
- Nogle modeller giver ikke nærmere oplysninger om udviklingsprocessen, strukturen og vurderingsmetoden
- Andre modeller og værktøjer, vi fandt, giver ingen nærmere oplysninger om strukturen og indholdet og er derfor ikke opført på listen
- Valget af modeller til gennemgang er baseret på geografisk dækning. Fokus vil primært være på modenhedsmodeller for cybersikkerhedskapacitet, der udarbejdes for at vurdere, hvordan de europæiske lande klarer sig. Det er imidlertid vigtigt at udvide den geografiske dækning for at analysere god praksis for opbygning af modenhedsmodeller i hele verden.

Denne systematiske gennemgang af relevante offentligt tilgængelige modenhedsmodeller for cybersikkerhedskapacitet blev gennemført ved hjælp af en tilpasset analyseramme, der er baseret på den metode, som Becker har defineret for udvikling af modenhedsmodeller[22]. Følgende elementer blev analyseret for hver eksisterende modenhedsmodel:

- **Navn på modenhedsmodel:** Navn på modenhedsmodel og de vigtigste referencer
- **Ansvarlig institution:** Den institution, uanset om den er offentlig eller privat, der er ansvarlig for udformningen af modellen
- **Generelt anvendelsesområde og mål:** Modellens overordnede anvendelsesområde og tilsigtede mål:
- **Antal og definition af niveauer:** Antal modenhedsniveauer i modellen og generel beskrivelse af disse
- **Antal attributter og navn på disse:** Antal og navn på attributter, som anvendes i modenhedsmodellen. Der er et tredobbelt formål med analysen af attributterne:
  - Opdeling af modenhedsmodellen i let forståelige afsnit
  - Samling af flere attributter i klynger af attributter, der opfylder samme mål
  - Angivelse af forskellige synsvinkler for modenhedsniveauet.
- **Vurderingsmetode:** Modenhedsmodellens vurderingsmetode
- **Præsentation af resultater**: Definere visualiseringsmetoden for resultaterne af modenhedsmodellen. Logikken bag dette skridt er, at modenhedsmodeller har en tendens

[22] J. Becker, R. Knackstedt og J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, s. 213–222, juni 2009.

til at ramme ved siden af, hvis de er for komplekse, og præsentationsmetoden skal derfor opfylde nogle praktiske behov.

Tidligere arbejde med NCSS

ENISA offentliggjorde to dokumenter om NCSS'er i 2012 som led i sin tidlige indsats. Først "Practical guide on the development and execution phase of NCSS"[23], der indeholder en række konkrete tiltag for effektivt at gennemføre en NCSS samt en præsentation af en NCSS' livscyklus i fire faser: strategisk udvikling, strategisk udførelse, strategisk evaluering og strategisk vedligeholdelse. Dernæst et dokument med overskriften "Setting the course for national efforts to strengthen security in cyberspace"[24], som redegjorde for status for cybersikkerhedsstrategier i og uden for EU i 2012 og foreslog, at medlemsstaterne skulle fastlægge fælles temaer og forskelle mellem deres NCSS'er.

Den første ENISA-ramme for evaluering af en medlemsstats NCSS blev offentliggjort i 2014[25]. Denne ramme indeholder anbefalinger og god praksis samt et sæt kapacitetsopbygningsværktøjer til evaluering af en NCSS (f.eks. klarlagte mål, input, resultater, centrale resultatindikatorer osv.). Disse værktøjer er tilpasset landenes forskellige behov på forskellige modenhedsniveauer i deres strategiske planlægning. Samme år offentliggjorde ENISA "Interactive Map Online NCSS Interactive Map"[26], som giver brugere mulighed for hurtigt at konsultere alle medlemsstaters og EFTA-landes NCSS'er, herunder deres strategiske mål og gode eksempler på gennemførelse. Kortet, der først blev udviklet som et NCSS-register (2014), blev ajourført med eksempler på gennemførelse i 2018, og siden 2019 har kortet fungeret som et *informationsknudepunkt* for centralisering af data fra medlemsstaterne om deres bestræbelser på at forbedre den nationale cybersikkerhed.

"NCSS Good Practice Guide"[27], der blev offentliggjort i 2016, udpeger femten strategiske mål. Denne vejledning analyserer også status for gennemførelse af hver medlemsstats NCSS og udpeger forskellige mangler og udfordringer i forbindelse med denne gennemførelse.

Efterfølgende offentliggjorde ENISA i 2018 "National Cybersecurity Strategies Evaluation Tool"[28]: et interaktivt selvvurderingsværktøj, der skal hjælpe medlemsstaterne med at evaluere deres strategiske prioriteter og mål i forbindelse med deres NCSS. Via en række enkle spørgsmål giver dette værktøj medlemsstaterne specifikke anbefalinger til gennemførelsen af hvert mål. Endelig introducerer "Good practices in innovation on Cybersecurity under the NCSS"[29], der blev offentliggjort i 2019, emnet innovation inden for cybersikkerhed under NCSS. Dokumentet beskriver udfordringer og god praksis på tværs af de forskellige innovationsaspekter, således som de opfattes af emneeksperter, med henblik på at bidrage til udarbejdelsen af fremtidige innovative strategiske mål.

A.1 Cybersecurity Capacity Maturity Model for Nations (CMM)

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, ajourført i 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Dette dokument er en ajourføring af vejledningen fra 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

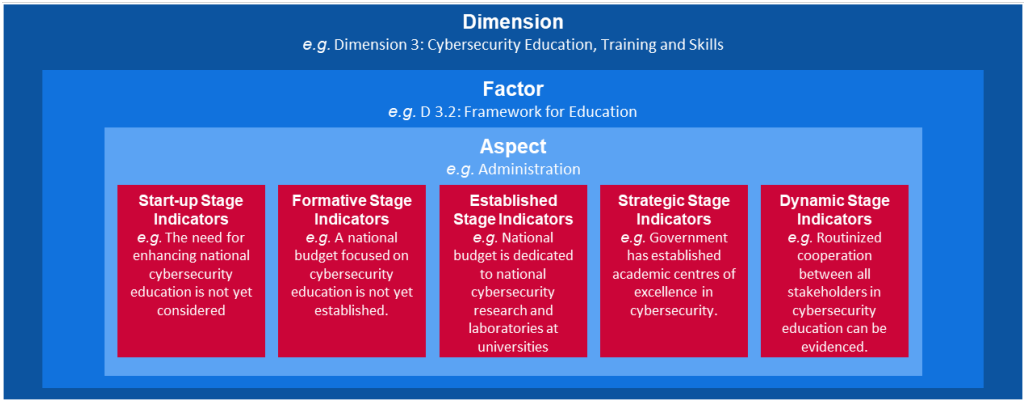
Cybersecurity Capacity Maturity Model for Nations (CMM) er udviklet af Global Cyber Security Capacity Centre (kapacitetscenter), der er en del af Oxford Martin School ved universitetet i Oxford. Formålet med kapacitetscentret er at øge omfanget og effektiviteten af kapacitetsopbygning inden for cybersikkerhed, både i Det Forenede Kongerige og internationalt, gennem anvendelse af Cybersecurity Capacity Maturity Model (CMM). CMM er direkte rettet mod lande, der ønsker at øge deres nationale cybersikkerhedskapacitet. CMM, der oprindeligt blev indført i 2014, blev revideret i 2016 efter dens anvendelse i forbindelse med gennemgangen af 11 nationale cybersikkerhedskapaciteter.

Attributter/dimensioner

I CMM antages cybersikkerhedskapacitet at omfatte **fem dimensioner**, der repræsenterer klyngerne i cybersikkerhed. Hver klynge repræsenterer forskellige "forskningsbriller" for undersøgelse og forståelse af cybersikkerhedskapacitet. Inden for de fem dimensioner beskrives detaljerne ved at råde over cybersikkerhedskapacitet gennem **faktorer**. Disse detaljer er elementer, der bidrager til at forbedre cybersikkerhedskapacitetens modenhed inden for hver dimension. Inden for hver faktor repræsenterer flere **aspekter** forskellige bestanddele af faktoren. Aspekterne repræsenterer en organisatorisk metode til at opdele indikatorerne i mindre klynger, som er lettere at forstå. Hvert aspekt evalueres derefter ved hjælp af **indikatorer** for at beskrive de trin, aktioner eller byggesten, der angiver et bestemt modenhedsniveau (defineret i næste afsnit) inden for et bestemt aspekt, en specifik faktor og en specifik dimension.

De begreber, der er nævnt ovenfor, kan inddeles som vist i figuren nedenfor.

Figur 4: Eksempel på CMM-indikatorer



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimension f.eks. dimension 3: Cybersikkerhedsuddannelse og -færdigheder
Factor e.g. D 3.2: Framework for Education	Faktor f.eks. D 3.2: Uddannelsesramme
Aspect e.g. Administration	Aspekt f.eks. administration
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indikatorer for opstartsfasen der er f.eks. endnu ikke overvejelser om at forbedre uddannelse inden for national cybersikkerhed
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indikatorer for forberedelsesfasen der er f.eks. endnu ikke fastlagt et nationalt budget med fokus på uddannelse i cybersikkerhed.
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indikatorer for den etablerede fase der er f.eks. vedtaget et nationalt budget for forskning i cybersikkerhed og laboratorier på universiteter

Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indikatorer for den strategiske fase f.eks. regeringens oprettelse af et akademisk ekspertisecenter inden for uddannelse i cybersikkerhed kan dokumenteres.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indikatorer for den dynamiske fase f.eks. standardiseret samarbejde mellem alle interessenter.

De fem dimensioner er beskrevet nedenfor:

i Udformning af cybersikkerhedspolitik og -strategi (6 faktorer)
ii Tilskyndelse til en ansvarlig cybersikkerhedskultur i samfundet (5 faktorer)
iii Udvikling af viden om cybersikkerhed (3 faktorer)
iv Etablering af effektive retlige og administrative rammer (3 faktorer)
v Risikostyring ved hjælp af standarder, organisationer og teknologier (7 faktorer).

Modenhedsniveauer

CMM anvender **5 modenhedsniveauer** til at afgøre, i hvilket omfang et land har gjort fremskridt med hensyn til en bestemt faktor/et bestemt aspekt af cybersikkerhedskapacitet. Disse niveauer giver et øjebliksbillede af den eksisterende cybersikkerhedskapacitet:

- **Opstartsfasen**: I denne fase er der enten ingen cybersikkerhedsmodenhed, eller den er meget lidt udviklet. Der kan være indledende drøftelser om kapacitetsopbygning inden for cybersikkerhed, men der er ikke truffet nogen konkrete foranstaltninger. I denne fase er der ikke nogen håndgribelig dokumentation.
- **Forberedelsesfasen**: Man kan begynde at registrere og formulere nogle karakteristika ved aspekterne, de kan være enkeltstående, ustrukturerede, dårligt definerede – eller simpelthen "nye". Der kan dog klart påvises dokumentation for denne aktivitet.
- **Den etablerede fase**: Elementerne i dette aspekt er på plads og fungerer. Der tages imidlertid ikke tilstrækkeligt hensyn til den forholdsmæssige fordeling af ressourcer. Der er kun truffet få beslutninger om udbyttet af de "forholdsmæssige" investeringer i de forskellige elementer i dette aspekt. Aspektet er imidlertid funktionelt og defineret.
- **Den strategiske fase**: Der er truffet valg om, hvilke dele af aspektet der er vigtige, og hvilke der er mindre vigtige for den pågældende organisation eller nation. Den strategiske fase afspejler det forhold, at disse valg er truffet, med forbehold for nationens eller organisationens særlige forhold.
- **Den dynamiske fase**: I denne fase er der klare mekanismer på plads til at ændre strategien afhængigt af de aktuelle omstændigheder, f.eks. teknologien i trusselsmiljøet, globale konflikter eller en væsentlig ændring inden for et område, der giver anledning til bekymring (f.eks. cyberkriminalitet eller privatlivets fred). Dynamiske organisationer har udviklet metoder til at ændre strategier på en afbalanceret måde. Hurtig beslutningstagning, omfordeling af ressourcer og konstant opmærksomhed på det skiftende miljø er kendetegnende for denne fase.

Vurderingsmetode

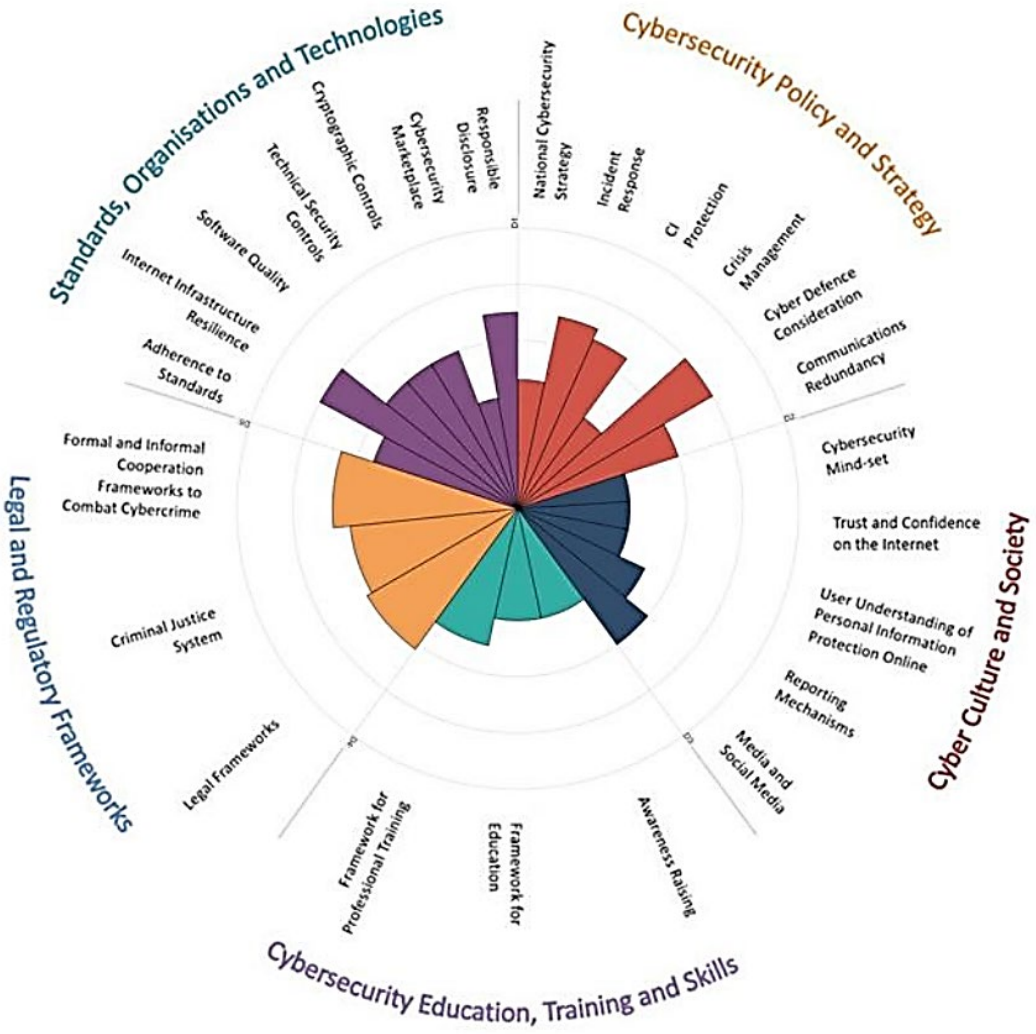
Da kapacitetscentret ikke har en detaljeret og indgående forståelse af hver national kontekst, som modellen anvendes i, arbejder det sammen med internationale organisationer, værtsministerier eller organisationer i det pågældende land for at gennemgå cybersikkerhedskapacitetens modenhed. For at vurdere modenhedsniveauet af de fem dimensioner, der indgår i CMM, mødes kapacitetscentret og værtsorganisationen med relevante nationale interessenter i den offentlige og private sektor over 2 eller 3 dage for at gennemføre fokusgrupper om dimensionerne af CMM'en. Hver dimension drøftes mindst to gange af forskellige grupper af interessenter. Dette udgør den foreløbige samling data, der ligger til grund for den efterfølgende vurdering.

Resultaternes form eller præsentation

CCM'en giver et overblik over modenhedsniveauet i det enkelte land via en radar bestående af fem afsnit, ét for hver dimension. Hver dimension repræsenterer en femtedel af grafikken, og de

fem modenhedsfaser for hver faktor strækker sig udad fra midten af grafikken. Som vist nedenfor er "opstartsfasen" tættest på grafikkens centrum, og "den dynamiske fase" er i den yderste kreds.

Figur 5 CMM: Resultatoversigt



Standards, Organisations and Technologies	Standarder, organisationer og teknologier
Legal Regulatory Frameworks	Retlige og administrative rammer
Cybersecurity Education, Training and Skills	Cybersikkerhedsuddannelse og -færdigheder
Cybersecurity Policy and Strategy	Cybersikkerhedspolitik og -strategi
Cyber Culture and Society	Cyberkultur og samfund
Responsible Disclosure	Ansvarlig videregivelse
Cybersecurity market place	Markedsplads for cybersikkerhed
Cryptographic Controls	Kryptografiske kontroller
Technical Security Controls	Teknisk sikkerhedskontrol
Software Quality	Softwarekvalitet
Internet Infrastructure Resilience	Modstandsdygtighed i internetinfrastruktur
Adherence to Standards	Overholdelse af standarder
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formelle og uformelle samarbejdsrammer for bekæmpelse af cyberkriminalitet
Criminal Justice System	Strafferetssystemet
Legal Frameworks	Retlige rammer

Framework for Professional Training	Ramme for erhvervsuddannelse
Framework for Education	Uddannelsesramme
Awareness Raising	Bevidstgørelse
Media and Social Medai	Medier og sociale medier
Reporting Mechanisms	Rapporteringsmekanismer
User Understanding of Personal Information Protection Online	Brugerforståelse af beskyttelse af personoplysninger online
Trust and Confidence on the Internet	Tiltro og tillid til internettet
Cybersecurity Mind-set	Cybersikkerhedstankegang
Communications Redundancy	Kommunikationsredundans
Cyber Defence Consideration	Overvejelser om cyberforsvar
Crisis Management	Krisestyring
CI Protection	Beskyttelse af CI
Incident Response	Beredskab
National Cybersecurity Strategy	National cybersikkerhedsstrategi

Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford, 2017.

A.2 Cybersecurity Capability Maturity Model (C2M2)

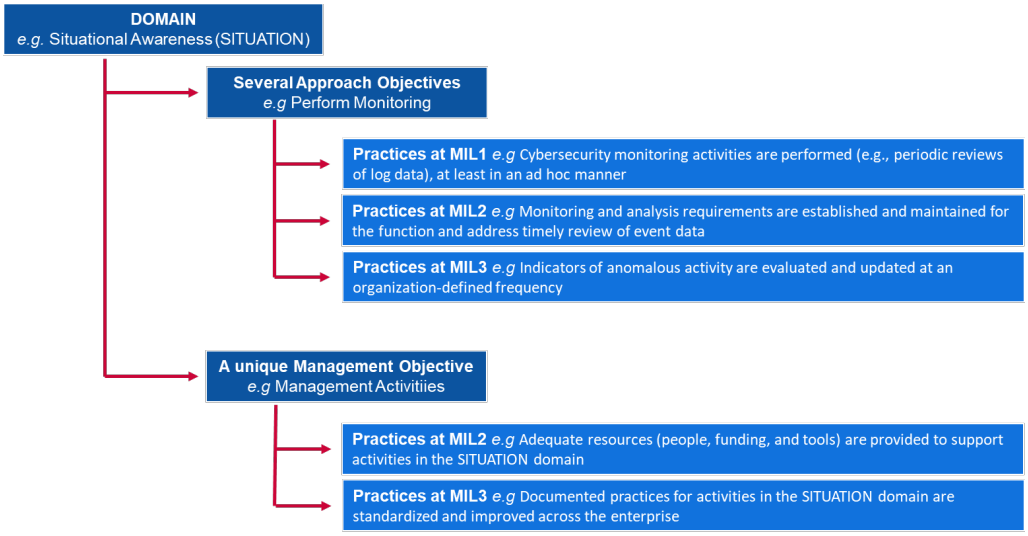
Cybersecurity Capacity Maturity Model (C2M2) er udviklet af det amerikanske energiministerium i samarbejde med eksperter fra den private og den offentlige sektor. Formålet med kapacitetscentret er at hjælpe organisationer i alle sektorer, af alle typer og enhver størrelse med at evaluere og forbedre deres cybersikkerhedsprogrammer og styrke deres operationelle modstandsdygtighed. C2M2 fokuserer på gennemførelsen og forvaltningen af cybersikkerhedspraksis i forbindelse med information, informationsteknologi (it) og driftsteknologiske (OT) aktiver samt de miljøer, de opererer i. C2M2 definerer modenhedsmodeller som: "et sæt karakteristika, attributter, indikatorer eller mønstre, der repræsenterer kapacitet og udvikling inden for en bestemt disciplin". C2M2 blev oprindeligt indført i 2014 og blev revideret i 2019.

Attributter/dimensioner

C2M2 behandler **ti områder**, der repræsenterer en logisk gruppering af cybersikkerhedspraksis. Hvert sæt af praksisser repræsenterer de aktiviteter, som en organisation kan udføre for at etablere og modne sin kapacitet på området. Hvert område forbindes derefter med et **unikt forvaltningsmål** og **flere mål for tilgangen**. Inden for både tilgangs- og forvaltningsmål er der anført **flere typer praksis** til at beskrive institutionaliserede aktiviteter.

Forholdet mellem disse begreber er opsummeret herunder:

Figur 6: Eksempel på C2M2-indikatorer



Domain eg Situational Awareness (SITUATION)	**Område**, f.eks. situationsbevidsthed (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring	**Mål med flere tilgange**, f.eks. udførelse af overvågning
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Praksis på MIL1**, f.eks. aktiviteter til overvågning af cybersikkerhed (f.eks. periodisk gennemgang af logdata), som minimum på ad hoc-basis
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Praksis på MIL2**, der er f.eks. fastlagt krav til overvågning og analyse, og de fastholdes med henblik på og rettidig gennemgang af hændelsesdata
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Praksis på MIL3**, f.eks. evalueres indikatorer for unormal aktivitet, og de opdateres med en hyppighed, der er fastlagt af organisationen
A unique Management Objectve e.g. Management Activities	Et unikt forvaltningsmål, f.eks. forvaltningsaktiviteter
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Praksis på MIL2**, f.eks. at der stilles tilstrækkelige ressourcer (mennesker, finansiering og værktøjer) til rådighed for at støtte aktiviteter inden for området SITUATION
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Praksis på MIL3**, f.eks. at dokumenteret praksis for aktiviteter på området SITUATION standardiseres og forbedres i hele virksomheden

De ti områder er beskrevet nedenfor:

i Risikostyring (RISKO)
ii Forvaltning af aktiver, ændringer og konfiguration (ASSET)
iii Identitets- og adgangsforvaltning (ACCESS)
iv Forvaltning af trusler og sårbarheder (THREAT)
v Situationsbevidsthed (SITUATION)
vi Hændelser og beredskab (RESPONSE)
vii Forvaltning af forsyningskæde og eksterne afhængighedsforhold (DEPENDENCIES)
viii Forvaltning af arbejdsstyrken (WORKFORCE)
ix Cybersikkerhedsarkitektur (ARCHITECTURE)
x Forvaltning af cybersikkerhedsprogrammer (PROGRAM).

Modenhedsniveauer

C2M2 anvender **fire modenhedsniveauer** (benævnt modenhedsindikatorniveauer – MIL) til at bestemme fremskridt på to planer, hvad angår modenhed: fremskridt inden for tilgang og forvaltning. MIL'erne går fra MIL0 til MIL3 og skal anvendes hver for sig for hvert domæne.

- **MIL0**: Praksis udføres ikke.
- **MIL1**: Indledende praksis udføres, men kan være ad hoc.
- **MIL2**: Forvaltningskarakteristika:
  - Praksis er dokumenteret
  - Der stilles tilstrækkelige ressourcer til rådighed til at støtte processen
  - Det personale, der udfører praksis, har tilstrækkelige færdigheder og viden
  - Ansvaret for og bemyndigelsen til at gennemføre praksis er tildelt.

  Karakteristika ved metode:
  - Praksis er mere fuldstændig eller avanceret end på MIL1.
- **MIL3**: Forvaltningskarakteristika:
  - Aktiviteter udføres i henhold til politikker (eller andre organisatoriske retningslinjer)

- Der er fastlagt resultatmål for områdeaktiviteter, og de overvåges med henblik på at følge resultater
- Dokumenteret praksis for områdeaktiviteter standardiseres og forbedres i hele virksomheden.

Karakteristika ved metode:

- Praksis er mere fuldstændig eller avanceret end på MIL2.

Vurderingsmetode

C2M2 er udformet til brug med en **selvvurderingsmetode** og værktøjskasse (som kan fås efter anmodning), så en organisation kan måle og forbedre sit cybersikkerhedsprogram. En selvvurdering ved hjælp af værktøjssættet kan færdiggøres på én dag, men værktøjssættet kan også tilpasses med henblik på en mere dybdegående evaluering. Desuden kan C2M2 anvendes som rettesnor for udviklingen af et nyt cybersikkerhedsprogram.

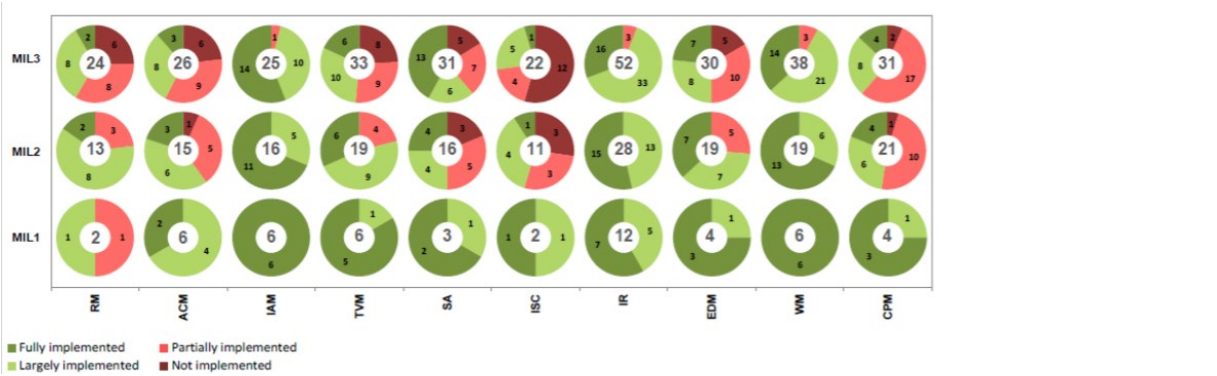
Modellens indhold præsenteres på et højt abstraktionsniveau, så det kan fortolkes af organisationer af forskellige typer, strukturer, størrelser og industrier. En udbredt anvendelse af modellen i en sektor kan understøtte benchmarking af sektorens cybersikkerhedskapacitet.

Resultaternes form eller præsentation

C2M2 indeholder en evalueringsrapport med scorer, der er genereret ud fra undersøgelsesresultaterne. I rapporten fremlægges resultaterne i to formater: det objektive format, hvor svar på spørgsmål vedrørende praksis fremlægges for hvert domæne og de tilhørende mål; og domæneformatet, hvor svar fremlægges for alle domæner og MIL'er. Begge formater er baseret på et præsentationssystem, der er karakteriseret ved cirkeldiagrammer (eller "donuts"), ét pr. svar, og en scoringsmekanisme baseret på trafiklyssystemet. Som vist i Figur 7 viser de røde sektorer i et cirkeldiagram en optælling af antal spørgsmål i undersøgelsen, hvor svaret var "ikke gennemført" (mørkerød) eller "delvist gennemført" (lyserød). De grønne sektorer viser antal spørgsmål, hvor svaret var "stort set gennemført" (lysegrøn) eller "fuldt gennemført" (mørkegrøn).

Figur 7 nedenfor er et eksempel på et scorekort ved afslutningen af en modenhedsvurdering. På X-aksen viser de 10 områder i C2M2, og Y-aksen angiver modenhedsniveauerne (MIL). I diagrammet er der for området risikostyring (RM) tre cirkeldiagrammer, hvor hvert cirkeldiagram svarer til et modenhedsniveau MIL1, MIL2 og MIL3 For området RM viser grafen, at der skal evalueres to elementer for at nå det første modenhedsniveau MIL1. I dette tilfælde er den ene score, "stort set gennemført", og én score "delvist gennemført". Med hensyn til det andet modenhedsniveau, MIL2, er der i modellen fastsat 13 elementer, der skal evalueres. To af disse 13 elementer hører til det første niveau, MIL1, og 11 til det andet niveau, MIL2. Det samme gælder for tredje niveau MIL3.

Figur 7: C2M2 – eksempel på domæneformat



Fully implemented	Kvalitetsstyringssystemet er implementeret
Largely implemented	Kvalitetsstyringssystemet er implementeret
Partially implemented	Delvist er gennemført
Not implemented	Kvalitetsstyringssystemet er implementeret
MIL1	MIL1:

MIL2	MIL2:
MIL3	MIL3:
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	TM
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Kilde: Det amerikanske energiministerium, Office of Electricity delivery and energy reliability, 2015.

A.3 Ramme for forbedring af cybersikkerhed i kritisk infrastruktur

Rammen for forbedring af cybersikkerhed i kritisk infrastruktur blev udviklet af det nationale institut for standarder og teknologi (NIST). Den fungerer som vejledning for cybersikkerhedsaktiviteter og risikostyring i en organisation. Den er rettet mod alle typer organisationer uanset størrelse, grad af cybersikkerhedsrisiko eller kompleksitet inden for cybersikkerhed. Da der er tale om en ramme og ikke en model, er den opbygget anderledes end de modeller, der er analyseret tidligere.

Rammen består af tre dele: rammens kerne, gennemførelsesniveauer og rammeprofilerne:

- **Rammens kerne** er et sæt cybersikkerhedsaktiviteter, ønskede resultater og gældende referencer, der er fælles for alle sektorer med kritisk infrastruktur. Disse svarer til de attributter eller dimensioner, der findes i modenhedsmodeller for cybersikkerhedskapacitet.
- **Rammens gennemførelseslag** ("lag") viser i hvilken sammenhæng, en organisation opfatter cybersikkerhedsrisici og de processer, der er indført for at styre denne risiko. Lagene, der går fra delvist (lag 1) til tilpasningsegnet (lag 4), beskriver en stigende grad af stringens og kompleksitet inden for risikostyringspraksis for cybersikkerhed. Lag repræsenterer ikke modenhedsniveauer, men har til formål at støtte organisatoriske beslutninger om, hvordan cybersikkerhedsrisici skal håndteres, og hvilke områder af organisationen, der har højere prioritet, og bør tildeles yderligere ressourcer.
- En **rammeprofil** ("profil") repræsenterer resultaterne baseret på de forretningsmæssige behov, som en organisation har valgt blandt rammekategorierne og underkategorierne. Profilen kan karakteriseres med hensyn til tilpasning af standarder, retningslinjer og praksis til rammens kerne i et bestemt gennemførelsesscenarie. Profiler kan anvendes til at identificere områder med muligheder for at forbedre status for cybersikkerhed ved at sammenligne en "aktuel" profil (status "som beset") med en "målprofil" ("kommende" status).

Rammens kerne

Rammens kerne består af fem **funktioner**. Når disse funktioner anvendes samlet, giver de et strategisk overblik på højt niveau af livscyklussen for en organisations håndtering af cybersikkerhedsrisici. Dernæst fastlægger rammens kerne underliggende centrale **kategorier** og **underkategorier** for hver funktion og matcher dem med eksempler på informative henvisninger såsom eksisterende standarder, retningslinjer og praksis for hver underkategori.

Funktioner og kategorier er beskrevet nedenfor:

i **Fastlægge**: Udarbejde en organisatorisk forståelse af, hvordan cybersikkerhedsrisici for systemer, mennesker, aktiver, data og kapaciteter håndteres.
- Underkategorier: Forvaltning af aktiver, erhvervsmiljø, ledelse, risikovurdering og strategi for risikostyring

ii **Beskytte:** Udvikle og gennemføre passende sikkerhedsforanstaltninger for at sikre levering af kritiske tjenester.

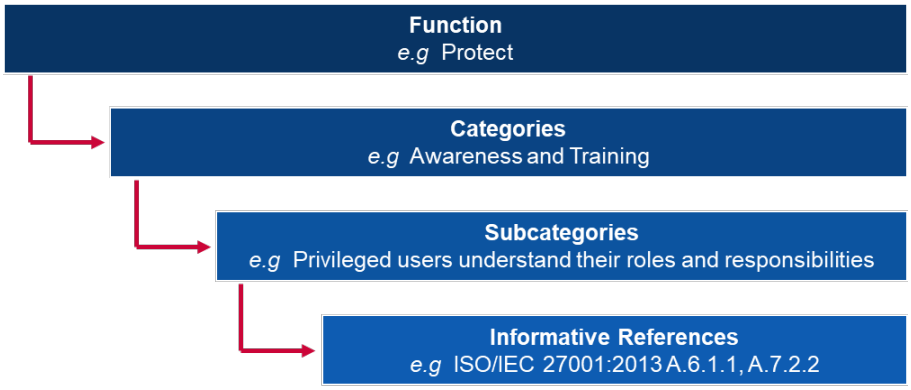
- Underkategorier: Identitetsforvaltning og adgangskontrol, bevidstgørelse og uddannelse, datasikkerhed, processer og procedurer for informationsbeskyttelse, vedligeholdelse og beskyttende teknologi

iii **Detektere:** Udvikle og gennemføre relevante aktiviteter for at identificere forekomsten af en cybersikkerhedshændelse.
- Underkategorier: Anomalier og hændelser, løbende sikkerhedsovervågning og detektionsprocesser

iv **Reagere:** Udvikle og gennemføre relevante aktiviteter for at træffe foranstaltninger vedrørende en detekteret cybersikkerhedshændelse.
- Underkategorier: Beredskabsplanlægning, kommunikation, analyse, afhjælpning og forbedringer.

v **Genoprette:** Udvikle og gennemføre passende aktiviteter med henblik på at opretholde planer for modstandsdygtighed og genoprette kapaciteter eller tjenester, der er blevet forringet som følge af en cybersikkerhedshændelse.
- Underkategorier: Genopretningsplanlægning, forbedringer og kommunikation

Figur 8: Eksempel på ramme for forbedring af cybersikkerhed i kritisk infrastruktur



Function e.g Project	**Funktion,** f.eks. et projekt
Categories e.g Awarness and Training	**Kategorier,** f.eks. bevidstgørelse og uddannelse
Subcategories e.g Privileged useres understand their roles and responsibilities	**Underkategorier,** f.eks. priviligerede brugeres forståelse af deres roller og ansvarsområder
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informative henvisninger,** f.eks. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Lag

Rammen for forbedring af cybersikkerhed i kritisk infrastruktur bygger på **4 lag**, som hver er defineret ved hjælp af tre akser: en risikostyringsproces, et integreret risikostyringsprogram og ekstern deltagelse. Lagene skal ikke betragtes som modenhedsniveauer, men som en ramme, der giver organisationerne mulighed for at anskue deres holdninger til cybersikkerhedsrisici i sammenhæng og de processer, der er indført for at styre denne risiko.

- **Lag 1: Delvis**
  - **Risikostyringsproces**: Praksis i organisationen for risikostyring i forbindelse med cybersikkerhed er ikke formaliseret, og risikoen forvaltes på ad hoc-basis og til tider reaktivt
  - **Integreret risikostyringsprogram**: Der er begrænset opmærksomhed på cybersikkerhedsrisici på organisationsniveau. Organisationen gennemfører risikostyring for cybersikkerhed på uregelmæssig og individuel basis og har eventuelt ikke indført processer, der gør det muligt at dele cybersikkerhedsoplysninger inden for organisationen
  - **Ekstern deltagelse**: Organisationen forstår ikke sin rolle i det større økosystem med hensyn til hverken afhængighedsforhold eller afhængighedsgrupper.

Organisationen er generelt ikke vidende om risici i cyberforsyningskæden for de produkter og tjenester, den leverer og anvender.

- **Lag 2: Information om risici**
  - **Risikostyringsproces**: Ledelsen har godkendt en risikostyringspraksis, men den er måske ikke indført som en politik, der gælder for hele organisationen.
  - **Integreret risikostyringsprogram**: Der er opmærksomhed på cybersikkerhedsrisici på organisationsniveau, men der er ikke fastlagt en organisatorisk tilgang til styring af cybersikkerhedsrisici. Cyberrisikovurdering af organisatoriske og eksterne aktiver forekommer, men kan typisk ikke gentages eller foretages kun én gang.
  - **Ekstern deltagelse**: Organisationen forstår generelt sin rolle i det større økosystem med hensyn til egne afhængighedsforhold eller afhængighedsgrupper, men ikke begge dele. Desuden er organisationen bekendt med de risici i cyberforsyningskæden, der er forbundet med de produkter og tjenester, den leverer og anvender, men den handler ikke konsekvent eller formelt i forbindelse med disse risici.
- **Lag 3: Repeterbar**
  - **Risikostyringsproces**: Organisationens risikostyringspraksis er formelt godkendt og formuleret som en politik. Organisatorisk cybersikkerhedspraksis ajourføres regelmæssigt på grundlag af risikostyringsprocesser for at medtage ændringer i forretnings-/missionskrav og ændringer i trussels- og teknologilandskabet.
  - **Integreret risikostyringsprogram**: Der er en organisatorisk tilgang til håndtering af cybersikkerhedsrisici. risikobaserede politikker, processer og procedurer defineres, gennemføres som aftalt og revideres siden. Den øverste ledelse sikrer, at cybersikkerhed er en indarbejdet faktor i alle organisationens aktivitetsområder.
  - **Ekstern deltagelse**: Organisationen forstår sin rolle, sine afhængighedsforhold og afhængighedsgrupper i det større økosystem og kan bidrage til samfundets bredere forståelse af risici. Organisationen er bekendt med risici i cyberforsyningskæden, der er relevante for de produkter og tjenester, den leverer og anvender.
- **Lag 4: Tilpasningsegnet**
  - **Risikostyringsproces**: Organisationen tilpasser sin cybersikkerhedspraksis i henhold til tidligere og nuværende cybersikkerhedsaktiviteter, herunder indhøstede erfaringer og prognoseindikatorer.
  - **Integreret risikostyringsprogram**: Der er en organisatorisk tilgang til styring af cybersikkerhedsrisici med inddragelse af risikobaserede politikker, processer og procedurer til håndtering af potentielle cybersikkerhedshændelser.
  - **Ekstern deltagelse**: Organisationen forstår sin rolle, sine afhængighedsforhold og afhængighedsgrupper i det større økosystem og bidrager til samfundets bredere forståelse af risici.

Vurderingsmetode

Rammen for forbedring af cybersikkerhed i kritisk infrastruktur er beregnet til, at organisationer selv kan vurdere deres risiko med henblik på at gøre deres cybersikkerhedstilgang og -investeringer mere rationelle, effektive og værdifulde. For at undersøge investeringernes effektivitet skal en organisation først have en klar forståelse af sine organisatoriske mål, forholdet mellem disse mål og understøttende cybersikkerhedsresultater. Cybersikkerhedsresultaterne af rammens kerne bidrager til selvvurdering af investeringers effektivitet og cybersikkerhedsaktiviteter.

A.4 Qatar Cybersecurity Capability Maturity Model (Q-C2M2)

Qatar Cybersecurity Capability Maturity Model (Q-C2M2) blev udviklet af det juridiske fakultet på universitetet i Qatar i 2018. Q-C2M2 er baseret på forskellige eksisterende modeller for at opbygge en omfattende vurderingsmetode til at forbedre Qatars ramme for cybersikkerhed.

Attributter/dimensioner

Q-C2M2 anvender det nationale institut for standarder og teknologis (NIST's) metode med fem kernefunktioner som de vigtigste områder i modellen. De fem kernefunktioner er anvendelige i Qatar, fordi de gælder for alle sektorer med kritisk infrastruktur, hvilket er et vigtigt element i

Qatars ramme for cybersikkerhed. Q-C2M2 er baseret på **fem områder**, der hver er inddelt i flere **delområder** for at dække hele spektret af cybersikkerhedskapacitetens modenhed.

De fem områder er beskrevet nedenfor:

i **Området forståelse** omfatter fire underområder: cyberstyring, aktiver, risici og uddannelse
ii Underområder under **området sikre** omfatter datasikkerhed, teknologisk sikkerhed, sikker adgangskontrol, sikker kommunikation og medarbejdersikkerhed
iii **Området eksponere** omfatter underområderne overvågning, håndtering af hændelser, detektion, analyse og eksponering
iv **Området reagere** omfatter beredskabsplanlægning, afhjælpning og beredskabskommunikation
v **Området opretholde** omfatter genopretningsplanlægning, kontinuitetsstyring, forbedring og eksterne afhængigheder.

Modenhedsniveauer

Q-C2M2 benytter **fem modenhedsniveauer** til måling af en statslig enheds eller en ikke-statslig organisations kapacitetsmodenhed for kernefunktionerne. Disse niveauer har til formål at vurdere modenhed inden for de fem områder, der er beskrevet i det foregående afsnit.

- **Indledende**: Anvender ad hoc-cybersikkerhedspraksis og -processer på nogle af områderne.
- **Gennemførelse**: Der er vedtaget politikker til at gennemføre alle cybersikkerhedsaktiviteter på områderne med henblik på at afslutte gennemførelsen på et bestemt tidspunkt.
- **Udvikling**: Der er gennemført politikker og praksisser, der skal udvikle og forbedre cybersikkerhedsaktiviteter på områderne med henblik på at foreslå nye aktiviteter, der skal gennemføres.
- **Tilpasningsegnet**: Cybersikkerhedsaktiviteter revideres og gennemgås, og praksis vedtages på baggrund af prognoseindikatorer udledt af tidligere erfaringer og foranstaltninger.
- **Fleksibel**: Tilpasningsfasen videreføres med øget vægt på fleksibilitet og hurtighed i forbindelse med gennemførelsen af aktiviteter på områderne.

Vurderingsmetode

Q-C2M2 befinder sig på et tidligt forskningsstadium og er endnu ikke klar til gennemførelse. Det er en ramme, der kan anvendes til at udføre en detaljeret vurderingsmodel for organisationer i Qatar i fremtiden.

A.5 Cybersecurity Maturity Model Certification (CMMC)

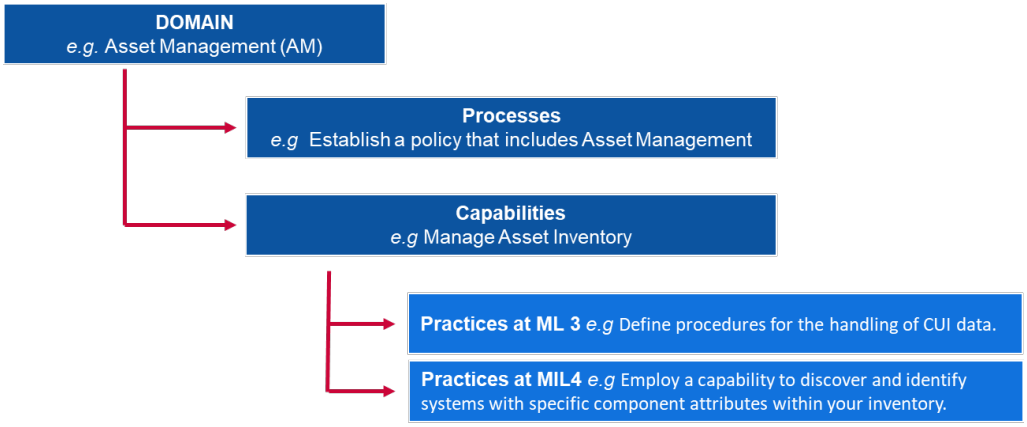
Cybersecurity Maturity Model Certification (CMMC) blev udviklet af det amerikanske forsvarsministerium i samarbejde med Carnegie Mellon University og Johns Hopkins University Applied Physics Laboratory. Det amerikanske forsvarsministeriums vigtigste mål for udformningen af denne model var at beskytte oplysninger fra forsvarsindustrien. De oplysninger, der vurderes i CMMC, klassificeres enten som "oplysninger i en kontrakt med staten", dvs. oplysninger, der stammer fra eller genereres til staten i henhold til en kontrakt, og som ikke er bestemt til offentliggørelse, eller "kontrollerede uklassificerede oplysninger", dvs. oplysninger, der kræver beskyttelse eller kontrol med formidling i henhold til og i overensstemmelse med love, forskrifter og statslige politikker. CMMC måler modenhedsniveauet af cybersikkerhed og leverer bedste praksis sammen med et certificeringselement for at sikre gennemførelsen af praksis i forbindelse med hvert modenhedsniveau. Den seneste udgave af CMMC blev offentliggjort i 2020.

Attributter/dimensioner

CMMC behandler **17 områder**, der repræsenterer klynger af cybersikkerhedsprocesser og -kapaciteter. Hvert område er opdelt i flere **processer**, der ligner hinanden på tværs af områder, og en eller flere **kapaciteter**, der omfatter fem modenhedsniveauer. Kapaciteterne (eller kapaciteten) er dernæst opdelt i **praksis** for hvert relevant modenhedsniveau.

Forholdet mellem disse begreber er vist nedenfor:

Figur 9: Eksempel på CMMC-indikatorer



DOMAIN e.g. Asset Management (AM)	**OMRÅDE**, f.eks. aktivstyring (AM)
Processes e.g Establish a policy that includes Asset Management	**Processer** f.eks. udforme en politik, der omfatter aktivstyring
Capabilities e.g Manage Asset Inventory	**Kapacitet** f.eks. styre aktivfortegnelse
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Praksis på MIL 3**, f.eks. definere procedurer til håndtering af CUI-data
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Praksis på MIL 4**, f.eks. anvende kapacitet til at opdage og udpege systemer med særlige komponentattributter i fortegnelsen.

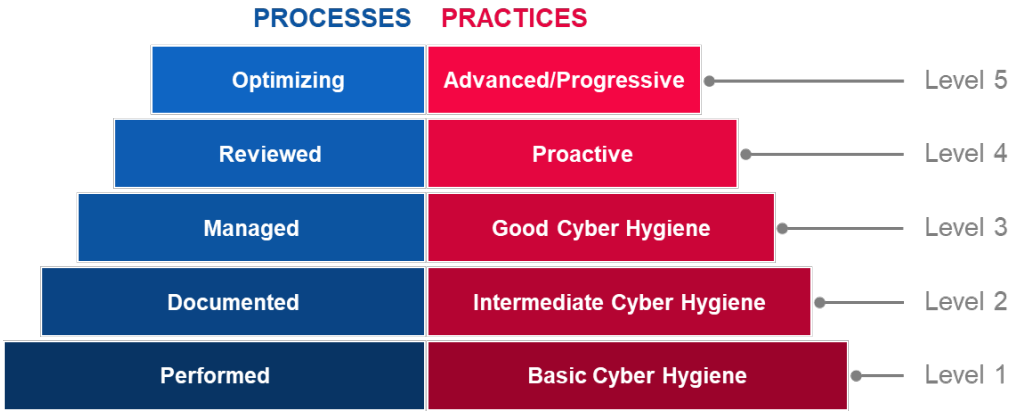
De 17 områder er beskrevet nedenfor:

i Adgangskontrol (AC)
ii Aktivstyring (AM)
iii Revision og pålidelighed (AU)
iv Bevidstgørelse og uddannelse (AT)
v Konfigurationsstyring (CM)
vi Identifikation og autentificering (IA)
vii Beredskab (IR)
viii Vedligeholdelse (MA)
ix Mediebeskyttelse (MP)
x Medarbejdersikkerhed (PS)
xi Fysisk beskyttelse (PE)
xii Genopretning (RE)
xiii Risikostyring (RM)
xiv Sikkerhedsvurdering (CA)
xv Situationsbevidsthed (SA)
xvi System- og kommunikationsbeskyttelse (SC)
xvii System- og informationsintegritet (SI).

Modenhedsniveauer

CMMC anvender **fem modenhedsniveauer**, der er defineret på grundlag af processer og praksis. For at opnå et vist modenhedsniveau i CMMC skal en organisation opfylde forudsætningerne for processerne og praksis for det pågældende niveau. Dette indebærer også opfyldelse af forudsætningerne for hele niveauet under det pågældende niveau.

Figur 10: Modenhedsniveauer i CMMC



PROCESSES	PROCESSER
Optimizing	Optimering
Reviewed	Gennemset
Managed	Administreret
Documented	Dokumenteret
Performed	Udført
PRACTICES	PRAKSIS
Advanced/Progressive	Avanceret/progressiv
Proactive	Proaktiv
Good Cyber Hygiene	God cyberhygiejne
Intermediate Cyber Hygiene	Middelgod cyberhygiejne
Basic Cyber Hygiene	Basal cyberhygiejne
Level 5	Niveau 5
Level 4	Niveau 4
Level 3	Niveau 3
Level 2	Niveau 2
Level 1	Niveau 1

- **Niveau 1**
  - **Processer – Udført:** Organisationen er måske kun i stand til at udføre denne praksis på ad hoc-basis og kan eller kan ikke henholde sig til dokumentation. Procesmodenhed vurderes ikke for niveau 1.
  - **Praksis – Grundlæggende cyberhygiejne**: På niveau 1 er fokus på beskyttelse af føderale oplysninger (FCI) og omfatter kun praksis, der svarer til grundlæggende beskyttelseskrav.
- **Niveau 2**
  - **Processer – Dokumenteret**: På niveau 2 er det et krav, at en organisation fastlægger og dokumenterer praksis og politikker for at vejlede gennemførelsen af dens CMMC-indsats. Dokumentation af praksis gør det muligt for enkeltpersoner at gentage praksis. Organisationer udvikler modenhedskapacitet ved at dokumentere deres processer og derefter anvende dem i henhold til dokumentationen.

- **Praksis – Middelgod cyberhygiejne**: Niveau 2 er en videreudvikling af niveau 1 på vej mod niveau 3 og omfatter en del af de sikkerhedskrav, der er specificeret i NIST SP 800-171, samt praksis fra andre standarder og referencer.

- **Niveau 3**
  - **Processer – Administreret**: På niveau 3 er det et krav, at en organisation udarbejder, vedligeholder og anvender en plan, der godtgør administration af aktiviteter til gennemførelse af praksis. Planen kan omfatte oplysninger om missioner, mål, projektplaner, ressourcer, obligatorisk uddannelse og inddragelse af relevante interessenter.
  - **Praksis – God cyberhygiejne**: På niveau 3 er fokus på beskyttelsen af CUI, og det omfatter alle de sikkerhedskrav, der er specificeret i NIST SP 800-171, samt yderligere praksis fra andre standarder og henvisninger for at afværge trusler.
- **Niveau 4**
  - **Processer – Revideret**: På niveau 4 er det et krav, at en organisation reviderer og måler effektiviteten af praksis. Ud over at måle effektiviteten af praksis er organisationer på dette niveau i stand til at træffe korrigerende foranstaltninger, når det er nødvendigt, og løbende informere den øverste ledelse om status eller forhold.
  - **Praksis – Proaktiv**: Niveau 4 fokuserer på beskyttelsen af CUI (kontrollerede uklassificerede oplysninger) og omfatter en undergruppe af de skærpede sikkerhedskrav. Denne praksis styrker en organisations detektions- og reaktionskapacitet i forhold til at håndtere og tilpasse sig skiftende taktikker, teknikker og procedurer.
- **Niveau 5**
  - **Processer – Optimering**: Niveau 5 kræver, at en organisation standardiserer og optimerer procesgennemførelsen i hele organisationen.
  - **Praksis – Avanceret/Proaktiv**: Niveau 5 fokuserer på beskyttelsen af CUI. Flere praksisser gør cybersikkerhedskapaciteten mere detaljeret og avanceret.

Vurderingsmetode

CMMC er en relativt ny model, som blev færdiggjort i første kvartal af 2020. Den er indtil nu ikke blevet anvendt i nogen organisation. Ikke desto mindre forventer det amerikanske forsvarsministeriums leverandører at kontakte certificerede tredjepartseksaminatorer med henblik på at gennemføre revisioner. Det amerikanske forsvarsministerium forventer, at leverandørerne gennemfører bedste praksis for at fremme cybersikkerhed og beskyttelse af følsomme oplysninger.

A.6 Community Cyber Security Maturity Model (CCSMM)

Community Cyber Security Maturity Model (CCSMM) blev udviklet af Centre for Infrastructure Assurance and Security på University of Texas. Formålet med CCSMM er bedre at definere metoder til at fastlægge den aktuelle status for et samfunds cyberberedskab og opstille en køreplan, som lokalsamfundene skal følge i deres forberedende arbejde. CCSMM er primært rettet mod lokalsamfund, der er lokale eller statslige myndigheder. CCSMM blev udformet i 2007.

Attributter/dimensioner

Modenhedsniveauer defineres i henhold til **seks hoveddimensioner,** der dækker de forskellige aspekter af cybersikkerhed i lokalsamfund og organisationer. Disse dimensioner er klart defineret for hvert modenhedsniveau (og er nærmere beskrevet i Figur 31: Oversigt over CCSMM). De seks dimensioner er:

i Imødegåelse af trusler
ii Parametre
iii Udveksling af oplysninger
iv Teknologi
v uddannelse

vi Afprøvning.

Modenhedsniveauer

CCSMM omfatter **fem modenhedsniveauer** baseret på de vigtigste typer af trusler og aktiviteter, der håndteres på det pågældende niveau:

- **Niveau 1: Sikkerhedsbevidst**
  Det primære tema for aktiviteter på dette niveau er at gøre enkeltpersoner og organisationer opmærksomme på trusler, problemer og spørgsmål vedrørende cybersikkerhed.
- **Niveau 2: Procesudvikling**
  Niveau, der skal hjælpe lokalsamfund med at etablere og forbedre de sikkerhedsprocesser, der er nødvendige for effektivt at håndtere cybersikkerhedsspørgsmål.
- **Niveau 3: Formidling af oplysninger**
  Dette niveau er udformet for at forbedre mekanismerne for udveksling af oplysninger inden for lokalsamfundet for at sætte det i stand til effektivt at sammenholde tilsyneladende uensartede oplysninger.
- **Niveau 4: Udvikling af taktik**
  Elementerne på dette niveau er udformet for at udvikle bedre og mere proaktive metoder til at opdage og reagere på angreb. På dette niveau bør de fleste forebyggelsesmetoder være på plads.
- **Niveau 5: Fuld operationel sikkerhedskapacitet**
  Dette niveau repræsenterer de elementer, der bør være på plads, for at enhver organisation kan betragte sig selv som fuldstændig parat på operationelt plan til at imødegå enhver form for cybertrussel.

Figur 31: Oversigt over CCSMM-dimensioner pr. niveau

	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1 Security Aware	Niveau 1 Sikkerhedsbevidst
Level 2 Process Development	Niveau 2 Procesudvikling
Level 3 Information Enabled	Niveau 3 Formidling af oplysninger
Level 4 Tactics Development	Niveau 4 Udvikling af taktik
Level 5 Full Security Operational Capability	Niveau 5 Fuld operationel sikkerhedskapacitet
Threats Addressed	Imødegåelse af trusler
Metrics	Parametre
Information sharing	Udveksling af oplysninger
Technology	Teknologi
Training	Uddannelse
Test	Afprøvning
Unstructured	Ustruktureret
Governement Industry Citizens	Stat Industri Borgere
Information Sharing Committee	Udvalg for Informationsudveksling
Rosters, GETS, Assess Controls, Encryption	Lister, GETS, adgangskontrol, kryptering
1-dat Community Seminar	Seminar i lokalsamfundet af 1 dags varighed
Dark Screen – EOC	Mørk skærm — EOC
Unstructured	Ustruktureret
Governement Industry Citizens	Stat Industri Borgere
Community Security Web site	Sikkerhed på lokalsamfundets hjemmeside
Secure Web Site Firewalls, Backups	Sikre firewalls, backups af hjemmeside
Conudcting a CCSE	Gennemførelse af en CCSE
Community Dark Screen	Mørk skærm i lokalsamfundet
Structured	Struktureret
Governement Industry Citizens	Stat Industri Borgere
Information Correlation Center	Informationskorrelationscenter
Event Correlation SW IDS/IPS	Hændelseskorrelation SW IDS/IPS
Vulnerability Assessment	Sårbarhedsvurdering
Operational Dark Screen	Operationel mørk skærm
Structured	Struktureret
Governement Industry Citizens	Stat Industri Borgere
State/Fed Correlation	Korrelation region/stat
24/7 manned operations	Døgnbemandede operationer
Operational Security	Operationel sikkerhed
Limited Black Demon	Begrænset sort behov
Highly Structured	Meget struktureret
Governement Industry Citizens	Stat Industri Borgere
Complete Info Vision	Fuldestgørende Info Vision
Automated Operations	Automatiske Operationer
Multi-Discipline Red Teaming	Multidisiplinær Red Teaming
Black Demon	Black Demon

Vurderingsmetode

CCSMM som vurderingsmetode skal anvendes af lokalsamfund med input fra statslige og føderale retshåndhævende myndigheder. Den har til formål at hjælpe lokalsamfund med at

definere, hvad der er vigtigst, hvilke der er de mest sandsynlige mål, og hvad der skal beskyttes (og i hvilket omfang). Med disse mål for øje kan der udarbejdes planer for at bringe hvert aspekt af lokalsamfundet op på det krævede niveau af cybersikkerhedsmodenhed. De specifikke oplysninger, der genereres af CCSMM, bidrager til at definere målene for forskellige afprøvninger og øvelser, der kan bruges til at måle effektiviteten af etablerede programmer.

A.7 Information Security Maturity Model for NIST's cybersikkerhedsramme (ISMM)

ISMM (Information Security Maturity Model) er udviklet af College of Computer Sciences and Engineering på universitetet King Fahd University of Petroleum and Minerals i Saudi-Arabien. Den foreslår en ny model for kapacitetsmodenhed til at måle gennemførelsen af cybersikkerhedsforanstaltninger. Formålet med ISMM er at sætte organisationerne i stand til at måle fremskridt i deres gennemførelse over tid ved regelmæssigt at anvende samme måleværktøj for at sikre, at den ønskede sikkerhedsstilling opretholdes. ISMM blev udviklet i 2017.

Attributter/dimensioner

ISMM bygger på de eksisterende vurderede områder i NIST-rammen og føjer en dimension til overensstemmelsesvurderingen. Dermed omfatter modellen **23 vurderede områder** vedrørende en organisations sikkerhedsstilling. De 23 vurderede områder er:

i Aktivstyring
ii Erhvervsmiljø
iii Ledelse
iv Risikovurdering
v Risikostyringsproces
vi Overensstemmelsesvurdering
vii Adgangskontrol
viii Bevidstgørelse og uddannelse
ix Datasikkerhed
x Informationsbeskyttelsesprocesser og -procedurer
xi Vedligeholdelse
xii Beskyttelsesteknologi
xiii Anomalier og hændelser
xiv Løbende sikkerhedsovervågning
xv Detektionsprocesser
xvi Beredskabsplanlægning
xvii Beredskabsmeddelelser
xviii Beredskabsanalyse
xix Beredskabsafhjælpning
xx Forbedringer af beredskab
xxi Genopretningsplanlægning
xxii Forbedringer af genopretning
xxiii Genopretning af meddelelser

Modenhedsniveauer

ISMM er baseret på **5 modenhedsniveauer**, som desværre ikke er beskrevet i den tilgængelige dokumentation.

- **Niveau 1:** Gennemført proces
- **Niveau 2:** Styret proces
- **Niveau 3:** Etableret proces
- **Niveau 4:** Forudsigelig proces
- **Niveau 5:** Optimering af processen.

Vurderingsmetode

ISMM foreslår ikke nogen specifik metode, som organisationer kan anvende til at foretage vurderingen.

A.8 Modellen for intern revisionskapacitet (IA- CM) for den offentlige sektor

Modellen for intern revisionskapacitet for den offentlige sektor (IA-CM) blev udviklet af Institute of Internal Auditors Research Foundation med henblik på at opbygge kapacitet og formidling gennem selvvurdering i den offentlige sektor. IA-CM, der henvender sig til revisionseksperter, giver et overblik over selve modellen samt en vejledning om anvendelse, der skal hjælpe med at bruge modellen som et selvvurderingsværktøj.

Selv om IA-CM er fokuseret på intern revisionskapacitet frem for kapacitetsopbygning inden for cybersikkerhed, er modellen opbygget som et selvvurderingsværktøj for enheder i den offentlige sektor, der kan anvendes globalt til at forbedre processer og effektivitet. Da anvendelsesområdet ikke er koncentreret om cybersikkerhed, vil attributterne ikke blive analyseret. IA-CM blev færdiggjort i 2009.

Modenhedsniveauer

Modellen for intern revisionskapacitet (IA-CM) omfatter **5 modenhedsniveauer**, som hver især beskriver karakteristikaene og kapaciteterne ved en intern revisionsaktivitet på dette niveau. Modellens kapacitetsniveauer udmunder i en køreplan for løbende forbedringer.

- **Niveau 1: Indledende**
  Ingen vedvarende, repeterbar kapacitet – afhængig af individuelle tiltag
  - Ad hoc eller ustruktureret
  - Isolerede enkeltstående revisioner eller gennemgange af dokumenter og transaktioner med henblik på nøjagtighed og overholdelse
  - Resultater, der afhænger af færdighederne hos den specifikke person, der beklæder stillingen
  - Der er ikke indført anden faglig praksis end den, der tilbydes af faglige sammenslutninger
  - Godkendelse af finansiering fra ledelsen efter behov
  - Mangel på infrastruktur
  - Revisorer vil sandsynligvis være en del af en større organisatorisk enhed
  - Der er ikke udarbejdet institutionel kapacitet.
- **Niveau 2: Infrastruktur**
  Bæredygtige og repeterbare praksisser og procedurer
  - Det centrale spørgsmål eller den centrale udfordring på niveau 2 er, hvordan processer gøres repeterbare, hvordan de fastholdes og dermed bliver til en repeterbar kapacitet
  - Interne revisionsrapporteringsrelationer, ledelsesmæssige og administrative infrastrukturer samt faglig praksis og processer er under udarbejdelse (intern revisionsvejledning, processer og procedurer)
  - Revisionsplanlægning er primært baseret på forvaltningsprioriteter
  - Der er fortsat stor afhængighed af specifikke personers færdigheder og kompetencer
  - Delvis overholdelse af standarderne.
- **Niveau 3: Integreret**
  Forvaltning og faglig praksis anvendes konsekvent
  - Interne revisionspolitikker, -processer og -procedurer er defineret, dokumenteret og indbyrdes integreret og integreret i organisationens infrastruktur.
  - Intern revisionsstyring og faglig praksis er veletableret og anvendes ensartet på tværs af den interne revisionsaktivitet.
  - Intern revision er ved at blive tilpasset organisationens virksomhed og de risici, den står over for.

- Intern revision udvikler sig fra kun at udføre traditionel intern revision til at blive integreret som holdspiller og yde rådgivning om resultater og risikostyring.
- Fokus er på teambuilding og aktiviteten i den interne revisionsfunktion samt dennes uafhængighed og objektivitet
- Generel overholdelse af standarderne.

- **Niveau 4: Administreret**

Integrerer oplysninger fra hele organisationen for at forbedre ledelsen og risikostyringen

- Der er overensstemmelse mellem intern revision og centrale interessenters forventninger.
- Der er indført resultatparametre til måling og overvågning af interne revisionsprocesser og -resultater.
- Intern revision anses for at yde væsentlige bidrag til organisationen.
- Interne revisionsfunktioner er en integreret del af organisationens ledelse og risikostyring.
- Intern revision er en velforvaltet forretningsenhed.
- Risici måles og håndteres kvantitativt.
- De nødvendige færdigheder og kompetencer er på plads med kapacitet til fornyelse og vidensdeling (inden for intern revision og på tværs af organisationen).

- **Niveau 5: Optimering**

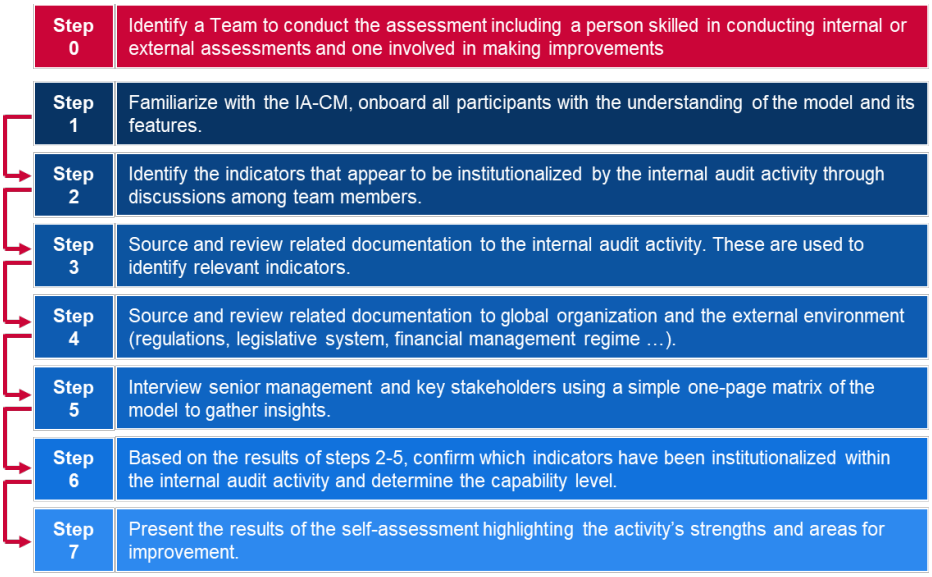
Læring i og uden for organisationen med henblik på løbende forbedring

- Intern revision er en læringsorganisation med løbende procesforbedringer og innovation.
- Intern revision benytter oplysninger inde fra og uden for organisationen til at bidrage til at nå strategiske mål.
- Resultater i verdensklasse/anbefalet/bedste praksis.
- Intern revision er en helt central del af organisationens ledelsesstruktur.
- Faglige og specialiserede kvalifikationer på højeste niveau.
- Præstationsmål på individuelt plan, enhedsplan og organisatorisk plan er fuldt integreret for at
- fremme præstationsforbedringer.

Vurderingsmetode

Modellen til intern revisionsfunktion er klart udarbejdet med henblik på selvvurdering. Den indeholder detaljerede skridt til brug af IA-CM og et eksempel på trin, der kan tilpasses. Inden selvvurderingen påbegyndes, skal der udpeges et specifikt team, hvor mindst én person er kvalificeret til at foretage interne eller eksterne vurderinger af interne revisioner, og én person der beskæftiger sig med forbedringer på dette område.

Figur 12: Trin i IC-AM-selvvurderingen



Step 0	Trin 0
Step 1	Trin 1
Step 2	Trin 2
Step 3	Trin 3
Step 4	Trin 4
Step 5	Trin 5
Step 6	Trin 6
Step 7	Trin 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Udpege et team, der skal foretage vurderingen, herunder en person, der er kvalificeret til at foretage interne eller eksterne vurderinger, og én person der beskæftiger sig med forbedringer.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Blive bekendt med IA-CM, introducere alle deltagere for og give dem en forståelse af modellen og dens karakteristika.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Kortlægge de indikatorer, der synes at blive institutionaliseret af den interne revisionsaktivitet gennem drøftelser blandt teammedlemmerne.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Indhente og gennemgå dokumentation vedrørende den interne revisionsaktivitet. Denne dokumentation anvendes til at kortlægge relevante indikatorer.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Indhente og gennemgå dokumentation vedrørende den globale organisation og det eksterne miljø (forordninger, lovgivningssystem, finansiel forvaltningsordning osv.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Gennemføre samtaler med den øverste ledelse og de vigtigste interessenter ud fra en 1-siders matrix i modellen for at indsamle viden.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	På grundlag af resultaterne af trin 2-5 bekræfte, hvilke indikatorer der er blevet institutionaliseret inden for den interne revisionsaktivitet, og fastlægge kapacitetsniveauet.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Fremlægge resultaterne af selvvurderingen med fokus på aktivitetens styrke og områder, hvor der kan ske forbedringer.

A.9 Globalt indeks for cybersikkerhed (GCI)

Det globale indeks for cybersikkerhed (GCI) er et initiativ fra Den Internationale Telekommunikationsunion (ITU), der har til formål at revidere tilsagn og status vedrørende cybersikkerhed i alle ITU-regioner: Afrika, Nord-, Syd- og Mellemamerika, de arabiske lande, Asien og Stillehavsområdet, SNG og Europa, og fremhæver lande med et stort engagement og anbefalet praksis. Målet med GCI er at hjælpe lande med at identificere områder, hvor der kan ske forbedringer inden for cybersikkerhed, og motivere dem til at træffe foranstaltninger til at forbedre deres placering og dermed bidrage til at højne det generelle cybersikkerhedsniveau på verdensplan.

Da GCI er et indeks og ikke nogen modenhedsmodel, anvender den ikke modenhedsniveauer, men derimod point til at indplacere og sammenligne nationers og regioners overordnede cybersikkerhedsforpligtelse.

Attributter/dimensioner

Det globale indeks for cybersikkerhed (GCI) er baseret på de fem søjler i den globale dagsorden for cybersikkerhed (GCA). Disse søjler udgør de fem delindekser i GCI og omfatter hver især et sæt indikatorer. De fem søjler og indikatorer er som følger:

i **Juridiske**: Mål baseret på eksisterende retlige institutioner og rammer, der beskæftiger sig med cybersikkerhed og cyberkriminalitet.
- Lovgivning om cyberkriminalitet
- Forskrifter om cybersikkerhed
- Lovgivning om inddæmning/begrænsning af spam.

ii **Tekniske**: Mål baseret på eksisterende tekniske institutioner og rammer, der beskæftiger sig med cybersikkerhed.
- CERT/CIRT/CSRIT
- Ramme for gennemførelse af standarder
- Standardiseringsorgan
- Tekniske mekanismer og kapaciteter, der anvendes til at bekæmpe spam
- Anvendelse af cloudcomputing til cybersikkerhedsformål
- Mekanismer til beskyttelse af børn online.

iii **Organisatoriske**: Mål baseret på eksisterende politiske koordineringsinstitutioner og strategier for udvikling af cybersikkerhed på nationalt plan.
- National cybersikkerhedsstrategi
- Ansvarligt agentur
- Cybersikkerhed.

iv **Kapacitetsopbygning**: Foranstaltninger baseret på eksisterende forskning og udvikling, uddannelses- og erhvervsuddannelsesprogrammer, certificerede fagfolk og offentlige agenturer, der fremmer kapacitetsopbygning.
- Offentlige oplysningskampagner
- Ramme for certificering og akkreditering af cybersikkerhedseksperter
- Faglige uddannelseskurser i cybersikkerhed
- Uddannelsesprogrammer eller akademiske læseplaner inden for cybersikkerhed
- FoU-programmer inden for cybersikkerhed
- Incitamentordninger.

v **Samarbejde:** Mål baseret på eksisterende partnerskaber, samarbejdsrammer og informationsdelingsnetværk.
- Bilaterale aftaler
- Multilaterale aftaler
- Deltagelse i internationale fora/sammenslutninger
- Offentlig-private partnerskaber
- Partnerskaber mellem/inden for agenturer
- Bedste praksisser.

Vurderingsmetode

GCI er et selvvurderingsværktøj, der er opbygget gennem en undersøgelse[30] af binære og åbne spørgsmål, der er kodet på forhånd. Anvendelsen af binære svar udelukker meningsbaseret evaluering og eventuelle forudindtagede holdninger til visse typer svar. Svar, der er kodet på forhånd, sparer tid og giver mulighed for en mere nøjagtig dataanalyse. Desuden giver en enkel dikotomisk skala mulighed for en hurtigere og mere kompleks evaluering, da den ikke kræver lange svar, hvilket fremskynder og strømliner processen med at svare og yderligere evaluering. Respondenten skal blot bekræfte tilstedeværelsen af eller manglen på visse på forhånd fastlagte cybersikkerhedsløsninger. En online undersøgelsesmetode, der anvendes til at

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

indsamle svar og uploade relevant materiale, gør det muligt at udlede god praksis og et sæt tematiske kvalitative evalueringer foretaget af et ekspertpanel.

Den overordnede GCI-proces gennemføres som følger:

- Der sendes en invitation til alle deltagere med information om initiativet og en anmodning om et kontaktpunkt med ansvar for at indsamle alle relevante data og udfylde online GCI-spørgeskemaet. Under onlineundersøgelsen opfordrer ITU officielt det godkendte kontaktpunkt til at besvare spørgeskemaet.
- Indsamling af primære data (for lande, der ikke besvarer spørgeskemaet):
  - ITU udarbejder et første udkast til besvarelse af spørgeskemaet ved hjælp af offentligt tilgængelige data og onlineundersøgelser
  - Udkastet til spørgeskema sendes til kontaktpunkterne med henblik på gennemgang
  - Kontaktpunkterne forbedrer nøjagtigheden og returnerer derefter udkastet til spørgeskema
  - Det korrigerede udkast til spørgeskema sendes til hvert kontaktpunkt til endelig godkendelse
  - Det godkendte spørgeskema anvendes til analyse, bedømmelse og indplacering.
- Indsamling af sekundære data (for lande, der besvarer spørgeskemaet):
  - ITU kortlægger eventuelt manglende svar, støttedokumenter, links osv.
  - Kontaktpunktet forbedrer eventuelt nøjagtigheden af svarene
  - Det korrigerede udkast til spørgeskema sendes til hvert kontaktpunkt til endelig godkendelse
  - Det godkendte spørgeskema anvendes til analyse, bedømmelse og indplacering.

A.10 Cyber Power Index (CPI)

Cyber Power Index (CPI) blev oprettet af forskningsprogrammet Economist Intelligence Unit og blev sponsoreret af Booz Allen Hamilton i 2011. CPI er en "dynamisk kvantitativ og kvalitativ model, [...] der måler specifikke attributter ved cybermiljøet på tværs af fire drivkræfter for cyberkraft: retlige og administrative rammer, økonomisk og social sammenhæng, teknologisk infrastruktur og anvendelse i industrien, som undersøger digitale fremskridt på tværs af centrale industrier"[31]. Formålet med Cyber Power Index er at benchmarke G20-landenes evne til at modstå cyberangreb og indføre den nødvendige digitale infrastruktur med henblik på at skabe en blomstrende og sikker økonomi. Det benchmark, der genereres af CPI, fokuserer på 19 lande i G20 (ekskl. EU). Indekset giver derefter en indplacering af landene for hver indikator.

Attributter/dimensioner

Cyber Power Index (CPI) er baseret på fire mekanismer for cyberpower. Hver kategori måles derefter ved hjælp af flere indikatorer for at give hvert land specifikke point. Der er følgende kategorier og søjler:

i **Retlig og administrativ ramme**
  - Statsligt engagement i cyberudvikling
  - Politikker om cyberbeskyttelse
  - Cybercensur (eller mangel herpå)
  - Politisk effektivitet
  - Beskyttelse af intellektuel ejendom

ii **Økonomisk og social kontekst**
  - Uddannelsesniveau
  - Tekniske færdigheder

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Åbenhed i samhandelen
- Innovationsgrad i forretningsmiljøet

iii **Teknologisk infrastruktur**

- Adgang til informations- og kommunikationsteknologi
- Kvalitet af informations- og kommunikationsteknologi
- Informations- og kommunikationsteknologi med lavere omkostninger
- Udgifter til informationsteknologi
- Antal sikre servere

iv **Anvendelse i industrien**

- Intelligente net
- E-sundhed
- E-handel
- Intelligent transport
- E-forvaltning

Vurderingsmetode

CPI er en kvantitativ og kvalitativ model til rangordning. Vurderingen blev foretaget af The Economist Intelligence Unit ved hjælp af kvantitative indikatorer fra tilgængelige statistiske kilder og ved at foretage skøn, når der manglede data. De vigtigste kilder var Economist Intelligence Unit, FN's Organisation for Uddannelse, Videnskab og Kultur (UNESCO), Den Internationale Telekommunikationsunion (ITU) og Verdensbanken.

A.11 Cyber Power Index (CPI)

I dette afsnit opsummeres de vigtigste resultater af analysen af de eksisterende modenhedsmodeller. Tabel 5: Oversigt over analyserede modenhedsmodeller giver et overblik over de vigtigste karakteristika ved hver model i henhold til den ændrede Becker-model. Tabel 6 Sammenligning af løbetidsniveauer beskriver de overordnede definitioner af de analyserede modellers modenhedsniveauer. Tabel 7 giver et overblik over de dimensioner eller attributter, der anvendes i hver model.

Tabel 5: Oversigt over analyserede modenhedsmodeller

Modelnavn	Ansvarlig institution	Formål	Mål	Antal niveauer	Antal attributter	Vurderingsmetode	Præsentation af resultater
Cybersecurity Capacity Maturity Model for Nations (CMM)	Center for global cybersikkerhedskapacitet University of Oxford	Øge omfanget og effektiviteten af kapacitetsopbygning inden for cybersikkerhed på internationalt plan	Lande	5	5 primære dimensioner	Samarbejde med en lokal organisation om at finjustere modellen, inden den anvendes i national sammenhæng	Radar med fem sektioner
Cybersecurity Capability Maturity Model (C2M2)	Det amerikanske energiministerium (DOE)	Bistå organisationer med at evaluere og forbedre deres cybersikkerhedsprogrammer og styrke deres operationelle modstandsdygtighed	Organisationer i alle sektorer, af enhver type og størrelse	4	10 primære områder	Metode og værktøjskasse til selvvurdering	Scorecard med cirkeldiagrammer
Ramme for forbedring af cybersikkerhed i kritisk infrastruktur	Det nationale institut for standarder og teknologi (NIST) (National Institute of Standards and Technology)	Ramme, der har til formål at fungere som vejledning for cybersikkerhedsaktiviteter og risikostyring i organisationer	Organisationer	Ikke tilgængelig (fire lag)	5 kernefunktioner	Selvvurdering	-
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	Det juridiske fakultet ved universitetet i Qatar	Levering af en brugbar model, der kan anvendes til at benchmarke, måle og udvikle Qatars cybersikkerhedsramme	Organisationer i Qatar	5	5 primære områder	-	-
Cybersecurity Maturity Model Certification (CMMC)	Det amerikanske forsvarsministerium (DOD)	Fremme bedste praksis for cybersikkerhed for at beskytte oplysninger	Organisationer inden for forsvarsindustrien	5	17 primære områder	Vurdering foretaget af tredjepartsrevisorer	-
Community Cybersecurity Maturity Model (CCSMM)	Centre for Infrastructure Assurance and Security, University of Texas	Fastlægge den aktuelle status for et samfunds cyberberedskab og opstille en køreplan, som lokalsamfund skal følge i deres forberedende arbejde	Lokalsamfund (lokale eller statslige forvaltninger)	5	6 primære dimensioner	Vurdering inden for lokalsamfund med input fra statslige og føderale retshåndhævende myndigheder	-
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	College of Computer Sciences and Engineering King Fahd University of Petroleum and, Minerals, Dhahran, Saudi-Arabien	Tillade organisationer at måle fremskridt i deres gennemførelse over tid for at sikre, at de opretholder den ønskede sikkerhedsstilling	Organisationer	5	23 vurderede områder	-	-
Modellen for intern revisionskapacitet (IA-CM) for den offentlige sektor	Institute of Internal Auditors Research Foundation	At opbygge intern revisionskapacitet og formidling gennem selvvurdering i den offentlige sektor.	Organisationer i den offentlige sektor	5	6 elementer	Selvevaluering	-
Globalt indeks for cybersikkerhed (GCI)	Den Internationale Telekommunikationsunion (ITU)	Revidere engagement i og status for cybersikkerhed og hjælpe lande med at identificere områder, hvor der kan ske forbedringer på cybersikkerhedsområdet	Lande	Ikke relevant	5 søjler	Selvvurdering	Rangordning

Cyber Power Index (CPI)	The Economist Intelligence Unit & Booz Allen Hamilton	Benchmarke G20-landenes evne til at modstå cyberangreb og indføre den nødvendige digitale infrastruktur med henblik på at skabe en blomstrende og sikker økonomi.	G20-landene	Ikke relevant	4 kategorier	Benchmarking foretaget af Economist Intelligence Unit	Prioriteringstabel

Tabel 6 Sammenligning af løbetidsniveauer

Model	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Cybersecurity Capacity Maturity Model for Nations (CMM)	**Opstartsfase** Enten er der ingen cybersikkerhedsmodenhed, eller den er meget lidt udviklet. Der kan være indledende drøftelser om kapacitetsopbygning inden for cybersikkerhed, men der er ikke truffet nogen konkrete foranstaltninger. I denne fase er der ikke nogen egentlig dokumentation.	**Forberedelsesfase** Man kan begynde at registrere og formulere nogle karakteristika ved aspekterne, de kan være enkeltstående, ustrukturerede, dårligt definerede – eller simpelthen "nye". Der kan dog klart påvises dokumentation for denne aktivitet.	**Oprettet** Elementerne i dette aspekt er på plads og fungerer. Der tages imidlertid ikke tilstrækkeligt hensyn til den forholdsmæssige fordeling af ressourcer. Der er kun truffet få beslutninger om udbyttet af de "forholdsmæssige" investeringer i de forskellige elementer i dette aspekt. Aspektet er imidlertid funktionelt og defineret.	**Strategisk** Der er truffet valg om, hvilke dele af aspektet der er vigtige, og hvilke der er mindre vigtige for den pågældende organisation eller nation. Den strategiske fase afspejler det forhold, at disse valg er truffet, med forbehold for forholdene i landet eller organisationen.	**Dynamisk** Der er indført klare mekanismer til at ændre strategien afhængigt af de aktuelle omstændigheder, f.eks. teknologien i trusselsmiljøet, globale konflikter eller en væsentlig ændring inden for et område, der giver anledning til bekymring (f.eks. cyberkriminalitet eller privatlivets fred). Dynamiske organisationer har udviklet metoder til at ændre strategier på en afbalanceret måde. Hurtig beslutningstagning, omfordeling af ressourcer og konstant opmærksomhed på det skiftende miljø er kendetegnende for denne fase.
Cybersecurity Capability Maturity Model (C2M2)	**MIL0:** Praksis udføres ikke.	**MIL1:** Indledende praksis udføres, men kan være ad hoc.	**MIL2:** Ledelseskarakteristika: Praksis er dokumenteret Der stilles tilstrækkelige ressourcer til rådighed til at støtte processen Det personale, der udfører praksis, har tilstrækkelige færdigheder og viden Ansvaret for og bemyndigelsen til at gennemføre praksis er tildelt. Karakteristika ved metode: Praksis er mere fuldstændig eller avanceret end på MIL1.	**MIL3:** Ledelseskarakteristika: Aktiviteter udføres i henhold til politikker (eller andre organisatoriske retningslinjer) Der er fastlagt resultatmål for områdeaktiviteter, og de overvåges med henblik på at følge resultater Dokumenteret praksis for områdeaktiviteter standardiseres og forbedres i hele virksomheden. Karakteristika ved metode: Praksis er mere fuldstændig eller avanceret end på MIL2.	-
Information Security Maturity Model for NIST's	**Gennemført proces**	**Styret proces**	**Etableret proces**	**Forudsigelig proces**	**Optimering af processen.**

cybersikkerhedsramme (ISMM)					
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	**Indledende** Anvender ad hoc-cybersikkerhedspraksis og -processer på nogle af områderne.	**Udvikling** Der er gennemført politikker og praksis med henblik på at udvikle og forbedre cybersikkerhedsaktiviteter på områderne med henblik på at foreslå nye aktiviteter, der skal gennemføres.	**Gennemførelse** Der er vedtaget politikker til at gennemføre alle cybersikkerhedsaktiviteter på områderne med henblik på at fuldføre gennemførelsen på et bestemt tidspunkt.	**Tilpasningsegnet** Cybersikkerhedsaktiviteter revideres og gennemgås, og der vedtages praksis på baggrund af prognoseindikatorer udledt af tidligere erfaringer og foranstaltninger.	**Fleksibel** Tilpasningsfasen videreføres med øget vægt på fleksibilitet og hurtighed i gennemførelsen af aktiviteter på områderne.
Cybersecurity Maturity Model Certification (CMMC)	**Processer: Udført** Fordi organisationen eventuelt kun er i stand til at udføre denne praksis på ad hoc-basis og eventuelt henholder sig til dokumentation, vurderes modenhedsniveau ikke for niveau 1. **Praksis: Grundlæggende cyberhygiejne** På niveau 1 er fokus på beskyttelse af FCI (oplysninger i en kontrakt med staten) og omfatter kun praksis, der svarer til grundlæggende beskyttelseskrav.	**Processer: Dokumenteret** På niveau 2 er det et krav, at en organisation fastlægger og dokumenterer praksis og politikker for at vejlede gennemførelsen af deres CMMC's indsats. Dokumentation af praksis gør det muligt for enkeltpersoner at gentage praksis. Organisationer udvikler modenhedskapacitet ved at dokumentere deres processer og derefter anvende dem i henhold til dokumentationen. **Praksis: Middelgod cyberhygiejne** Niveau 2 er en videreudvikling af niveau 1 på vej mod niveau 3 og omfatter en del af de sikkerhedskrav, der er specificeret i NIST SP 800-171, samt praksis fra andre standarder og referencer.	**Processer: Administreret** På niveau 3 er det et krav, at en organisation udarbejder, vedligeholder og anvender en plan, der godtgør administration af aktiviteter til gennemførelse af praksis. Planen kan omfatte oplysninger om missioner, mål, projektplaner, ressourcer, obligatorisk uddannelse og inddragelse af relevante interessenter. **Praksis: God cyberhygiejne**. På niveau 3 er fokus på beskyttelsen af CUI (kontrollerede uklassificerede oplysninger), og det omfatter alle de sikkerhedskrav, der er specificeret i NIST SP 800-171, samt yderligere praksis fra andre standarder og henvisninger for at afbøde trusler.	**Processer: Revideret.** På niveau 4 er det et krav, at en organisation reviderer og måler effektiviteten af praksis. Ud over at måle effektiviteten af praksis er organisationer på dette niveau i stand til at træffe korrigerende foranstaltninger, når det er nødvendigt, og løbende informere den øverste ledelse om status eller problemer. **Praksis: Proaktiv** Niveau 4 fokuserer på beskyttelsen af CUI (kontrollerede uklassificerede oplysninger) og omfatter en undergruppe af de skærpede sikkerhedskrav. Denne praksis styrker en organisations detektions- og reaktionskapacitet i forhold til at håndtere og tilpasse sig skiftende taktikker, teknikker og procedurer.	**Processer: Optimering** På niveau 5 er det et krav, at en organisation standardiserer og optimerer procesgennemførelsen i hele organisationen. **Praksis: Avanceret/Proaktiv** Niveau 5 fokuserer på beskyttelse af CUI (kontrollerede uklassificerede oplysninger). Flere praksisser gør cybersikkerhedskapaciteten mere detaljeret og avanceret.
Community Cyber Security Maturity Model (CCSMM)	**Sikkerhedsbevidsthed** Det primære tema for aktiviteter på dette niveau er at gøre enkeltpersoner og organisationer opmærksomme på trusler, problemer og spørgsmål vedrørende IT-sikkerhed.	**Procesudvikling** Niveau, der skal hjælpe lokalsamfund med at etablere og forbedre de sikkerhedsprocesser, der er nødvendige for effektivt at håndtere cybersikkerhedsspørgsmål.	**Formidling af oplysninger** Dette niveau er udformet for at forbedre mekanismerne for udveksling af oplysninger inden for lokalsamfundet for at sætte det i stand til effektivt at sammenholde tilsyneladende uensartede oplysninger.	**Udvikling af taktik** Elementerne på dette niveau er udformet for at udvikle bedre og mere proaktive metoder til at opdage og reagere på angreb. På dette niveau bør de fleste forebyggelsesmetoder være på plads.	**Fuld operationel sikkerhedskapacitet** Dette niveau repræsenterer de elementer, der bør være på plads, for at enhver organisation kan betragte sig selv som fuldstændig parat på operationelt plan til at imødegå enhver form for cybertrussel.

Modellen for intern revisionskapacitet (IA- CM) for den offentlige sektor	**Grundlæggende** Ingen vedvarende, repeterbar kapacitet – afhængig af individuelle tiltag	**Infrastruktur** Bæredygtige og repeterbare praksisser og procedurer	**Integreret** Forvaltning og faglig praksis anvendes konsekvent	**Administreret** Indarbejder oplysninger fra hele organisationen for at forbedre ledelsen og risikostyringen	**Optimering** Læring i og uden for organisationen med henblik på løbende forbedring

Tabel 7: Sammenligning af attributter/dimensioner

	Cybersecurity Capacity Maturity Model for Nations (CMM)	Cybersecurity Capability Maturity Model (C2M2)	Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	Cybersecurity Maturity Model Certification (CMMC)	Cybersecurity Maturity Model Certification (CMMC)	Information Security Maturity Model for NIST's cybersikkerhedsramme (ISMM)	Ramme for forbedring af cybersikkerhed i kritisk infrastruktur	Globalt indeks for cybersikkerhed (GCI)	Cyber Power Index (CPI)
Niveauer	Fem dimensioner, der igen er inddelt i flere faktorer, herunder flere aspekter og indikatorer (Figur 4)	Ti domæner, herunder et unikt ledelsesmål og flere objektive tilgange (Figur 6)	Fem domæner opdelt i underdomæner	17 domæner opdelt i processer og én til flere kapaciteter, som igen opdeles i forskellige praksisser (Figur 9).	Seks primære dimensioner	23 vurderede områder	Fem funktioner med underliggende nøglekategorier og underkategorier (Figur).	Fem søjler, herunder flere indikatorer	Fire kategorier med flere indikatorer
Attributter/dimensioner	i Udformning af cybersikkerhedspolitik og -strategi ii Tilskyndelse til en ansvarlig cybersikkerhedskultur i samfundet iii Udvikling af viden om cybersikkerhed iv Etablering af effektive retlige og administrative rammer v Risikostyring ved hjælp af standarder, organisationer og teknologier.	i Risikostyring ii Forvaltning af aktiver, ændringer og konfiguration iii Identitets- og adgangsforvaltning iv Forvaltning af trusler og sårbarheder v Situationskendskab vi Hændelser og beredskab vii Forvaltning af forsyningskæde og eksterne afhængighedsforhold viii Forvaltning af arbejdsstyrken ix Cybersikkerhedsarkitektur x Forvaltning af cybersikkerhedsprogrammer.	i Forståelse (cyberstyring, aktiver, risici og uddannelse) ii Sikkerhed (datasikkerhed, teknologisk sikkerhed, sikker adgangskontrol, sikker kommunikation og medarbejdersikkerhed) iii Eksponering (overvågning, hændelseshåndtering, detektion, analyse og eksponering) iv Beredskab (beredskabsplanlægning, afhjælpning og beredskabskommunikation) v Opretholde (genopretningsplanlægning, kontinuitetsstyring, forbedring og eksterne afhængigheder).	i Adgangskontrol ii Aktivstyring iii Revision og ansvarlighed iv Bevidstgørelse og uddannelse v Konfigurationsstyring vi Identifikation og autentificering vii Beredskab viii Vedligeholdelse ix Mediebeskyttelse x Personalesikkerhed xi Fysisk beskyttelse xii Genopretning xiii Risikostyring xiv Sikkerhedsvurdering xv Situationskendskab xvi System- og kommunikationsbeskyttelse xvii System- og informationsintegritet.	i Imødegåelse af trusler ii Parametre iii Udveksling af oplysninger iv Teknologi v Uddannelse vi Afprøvning	i Aktivstyring ii Erhvervsmiljø iii Ledelse iv Risikovurdering v Risikostyringsproces vi Overensstemmelsesvurdering vii Adgangskontrol viii Bevidstgørelse og uddannelse ix Datasikkerhed x Informationsbeskyttelsesprocesser og -procedurer xi Vedligeholdelse xii Beskyttelsesteknologi xiii Anomalier og hændelser xiv Løbende sikkerhedsovervågning xv Detektionsprocesser xvi Beredskabsplanlægning xvii Beredskabsmeddelelser xviii Beredskabsanalyse xix Beredskabsafhjælpning xx Forbedringer af beredskab xxi Genopretningsplanlægning xxii Forbedringer af genopretning xxiii Genopretning af meddelelser	i Fastlægge ii Beskytte iii Detektere iv Reagere v Genoprette	i Juridisk ii Teknisk iii Organisatorisk iv Kapacitetsopbygning v Samarbejde.	i Retlig og administrativ ramme ii Økonomisk og social kontekst iii Teknologisk infrastruktur iv Anvendelse i industrien.

BILAG B – LITTERATURLISTE TIL DOKUMENTATIONSUNDERSØGELSEN

Almuhammadi, S. og Alsaleh, M. (2017) "Information Security Maturity Model for Nist Cyber Security Framework", i Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. og Alsaleh, M. (2017) "Information Security Maturity Model for Nist Cyber Security Framework", i Computer Science & Information Technology (CS & IT). Findes på: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Findes på: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Findes på: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) "Introduction to Return on Security Investment".

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) “Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Findes på https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Findes på: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity - Self-assessment Tool (uden dato). Findes på: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011) Specialised cybercrime units - Good practice study. Findes på: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (uden dato). Findes på: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Cyperns kommissær med ansvar for elektronisk kommunikation og postvæsen (2012) Cybersecurity Strategy of the Republic of Cyprus.

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (uden dato) "Welcome to the NCSS Training Tool".

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Findes på: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Findes på: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Findes på: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Den belgiske regerings cybersikkerhedsstrategi (2012). Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Den bulgarske regering (2015) National Cyber Security Strategy - Cyber-resistant Bulgaria 2020.

Den danske regering - finansministeriet (2018) Danish Cyber and Information Security Strategy. Findes på: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (2017) Handbook on security of personal data processing. Findes på: http://dx.publications.europa.eu/10.2824/569768

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Findes på: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Den Europæiske Unions Tidende (2008) RÅDETS DIREKTIV 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre. Findes på: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Den franske premierministers kontor (2014) French National Digital Security Strategy. Findes på: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Den Internationale Telekommunikationsunion (ITU) (2018) Guide to developing a national cybersecurity strategy. Findes på: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Den Internationale Telekommunikationsunion (ITU) (2018) The Global Cybersecurity Index. Findes på: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Den nederlandske regering (2018) National Cybersecurity Agenda. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Den rumænske regering (2013) Cyber security strategy of Romania. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Den slovakiske regering (2015) Cyber Security Concept of the Slovak Republic. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Den svenske regering (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Det Europæiske Agentur for Net- og Informationssikkerhed (2012 NCSS: Practical Guide on Development and Execution. Heraklion: ENISA

Det Europæiske Agentur for Net- og Informationssikkerhed (2012 NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA

Det Europæiske Agentur for Net- og Informationssikkerhed (2016) Guidelines for SMEs on the security of personal data processing.

Det Europæiske Agentur for Net- og Informationssikkerhed (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA

Det Hvide Hus (2018) National Cyber Strategy of the United States of America. Findes på: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Det portugisiske ministerråd (2019), Den Portugisiske Republiks statstidende, serie 1 – nr. 108 – Ministerrådets resolution nr. 92/2019. Findes på: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Det schweiziske forbundsråd (2018) National strategy for the protection of Switzerland against cyber risks.

Det tyske forbundsindenrigsministerium (2011) Cyber Security Strategy for Germany. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Digital Slovenia (2016) Cybersecurity Strategy. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Europa-Kommissionen (2012) Europa-Parlamentets og Rådets forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. Findes på: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Findes på: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Den Europæiske Union og Det Europæiske Agentur for Net- og Informationssikkerhed (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Foreningen af Interne Revisorer (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Formandskabet for det italienske ministerråd (2017) The Italian Cybersecurity Action Plan. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) "Evaluating Business Process Maturity Models", Journal of the Association for Information Systems. Findes på: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Grækenlands regering (2017) National Cyber Security Strategy. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Irlands regering (2019) National Cyber Security Strategy. Findes på: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

J.D., R. D. B. (2019) "Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework", International Review of Law.

Kroatiens regering (2015) The National Cyber Security Strategy of The Republic of Croatia. Findes på: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Letlands regering (2014) Cyber Security Strategy of Latvia. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Luxembourgs regeringsråd (2018) National Cybersecurity Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministry for Competitiveness and Digital, Maritime and Services Economy (2016) Malta Cyber Security Strategy. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

National Cyber Security Strategies - Interactive Map (uden dato). Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018) Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology Findes på: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Findes på: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Den Europæiske Union og Det Fælles Forskningscenter - Europa-Kommissionen (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Findes på: https://www.oecd.org/sdd/42495745.pdf.

Organisationen for Økonomisk Samarbejde og Udvikling (OECD) (2012) Cybersecurity policy making at a turning point. Findes på: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) "National Cyber Security Strategies - Practical Guide on Development and Execution".

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Findes på: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Republikken Estlands ministerium for økonomiske anliggender og kommunikation (2019) Cybersecurity Strategy – Republic of Estonia. Findes på: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Republikken Litauens forsvarsministerium (2018) National Cyber Security Strategy

Republikken Tjekkiets nationale center for cybersikkerhed (2015) National Cyber Security Strategy of the Czech Republic. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Republikken Østrigs forbundskancelli (2013) Austrian Cyber Security Strategy. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Sarri, A., Kyranoudi, P. og Den Europæiske Unions Agentur for Cybersikkerhed (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Findes på: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Sikkerhedsudvalgets sekretariat (2019) Finland's Cyber Security Strategy 2019. Findes på: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Smith, R. (2015) Europa-Parlamentets og Rådets direktiv 2010/41/EU af 7. juli 2010

Smith, R. (2016) "Europa-Parlamentets og Rådets direktiv 2010/41/EU af 7. juli 2010", i Smith, R., Core EU Legislation. London: Macmillan Education. Findes på: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Spaniens regering (2019) National Cyber Security Strategy. Findes på: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Trimintzios, P., et al. (2011) Cyber Europe Report. Findes på: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report.* Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Findes på: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021 (2016). Findes på: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Ungarns regering (2018) Strategy for the Security of Network and Information Systems. Findes på: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

University of Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) 'ITU National Cybersecurity Strategy Guide. Findes på: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) "The Community Cyber Security Maturity Model", i 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

BILAG C – ANDRE UNDERSØGTE MÅL

De mål, der er beskrevet nedenfor, blev undersøgt som led i dokumentationsundersøgelsen og de interview, der blev gennemført af ENISA. Følgende mål er ikke en del af rammen for vurdering af national kapacitet, men de kaster lys over emner, som det er værd at drøfte. Hvert af de følgende underkapitler indeholder en redegørelse for, hvorfor målet ikke blev medtaget.

- Udvikle sektorspecifikke cybersikkerhedsstrategier
- Bekæmpe misinformationskampagner
- Sikre banebrydende teknologier (5G, AI, kvantedatabehandling...)
- Sikre datasuverænitet
- Give incitamenter til udvikling af cyberforsikringsbranchen.

Udvikle sektorspecifikke cybersikkerhedsstrategier

Vedtagelsen af sektorspecifikke strategier, der er rettet mod tiltag og -incitamenter i bestemte sektorer, introducerer uden tvivl en stærkere decentraliseret kapacitet. Dette gælder navnlig for medlemsstater, hvis OES'er skal håndtere forskellige rammer og regler, og hvor der er mange afhængigheder, fordi cybersikkerhed er relevant på alle planer. I flere medlemsstater er der almindeligvis mange nationale myndigheder og tilsynsorganer med kendskab til de særlige forhold i hver enkelt sektor, og som har mandat til at håndhæve specifikke bestemmelser for hver sektor.

Danmark lancerede f.eks. seks målrettede strategier for de mest kritiske sektorers cyber- og informationssikkerhedsindsats for at udvikle en stærkere decentraliseret kapacitet inden for cyber- og informationssikkerhed. Hver "sektorenhed" vil bidrage til bl.a. trusselsvurderinger på sektorniveau, overvågning, beredskabsøvelser, etablering af sikkerhedssystemer, videndeling og instrukser. De sektorspecifikke strategier omfatter følgende sektorer:

- Energi
- Sundhedspleje
- Transport
- Telekommunikation
- Økonomi
- Det maritime område.

Andre medlemsstater har udtrykt interesse for at overveje sektorspecifikke cybersikkerhedsstrategier for at afspejle alle lovgivningsmæssige krav. Det skal dog påpeges, at et sådant mål eventuelt ikke er egnet til alle medlemsstater afhængigt af deres størrelse, nationale politikker og modenhed. De store udfordringer ved at sikre, at rammen kan tage højde for alle særlige forhold, betød, at ENISA ikke medtog dette mål i rammen.

Bekæmpe misinformationskampagner

Medlemsstaterne integrerer beskyttelsen af grundlæggende principper såsom menneskerettigheder, gennemsigtighed og offentlighedens tillid i deres nationale cybersikkerhedsstrategier. Dette er meget vigtigt, især hvad angår misinformation, der udbredes via traditionelle nyhedsmedier eller sociale medieplatforme. Derudover er cybersikkerhed i øjeblikket en af de største udfordringer i forbindelse med valg. Der er i flere lande forud for

vigtige valg blevet registreret aktiviteter som f.eks. udbredelse af falske oplysninger eller negativ propaganda. Denne trussel har potentiale til at underminere EU's demokratiske proces. På europæisk plan har Kommissionen udarbejdet en handlingsplan[32] for at fremskynde bestræbelserne på at bekæmpe misinformation i Europa: denne plan fokuserer på fire centrale områder (detektion, samarbejde, samarbejde med onlineplatforme og bevidstgørelse) og har til formål at opbygge EU's kapacitet og styrke samarbejdet mellem medlemsstaterne.

4 ud af 19 interviewede lande har givet udtryk for, at de har til hensigt at tackle problemet med misinformation og propaganda i deres NCSS.

I den franske NCSS[33] hedder det f.eks., at: "Det er statens ansvar at informere borgerne om risikoen for manipulation og propagandateknikker, der anvendes af ondsindede aktører på internettet. Efter terrorangrebene mod Frankrig i januar 2015 oprettede regeringen f.eks. en informationsplatform om risiciene i forbindelse med islamisk radikalisering via elektroniske kommunikationsnet: "Stop-djihadisme.gouv.fr"." Denne tilgang kan udvides til at reagere på andre eksempler på propaganda eller destabilisering.

I et andet eksempel, Polens NCSS for 2019-2024[34], fremgår det, at: "Over for manipulerende aktiviteter, såsom misinformationskampagner er der behov for systemiske indsatser for at gøre borgere opmærksomme på kontrol af oplysningernes ægthed og reaktion på forsøg på at forvride dem."

Under de interview, som ENISA gennemførte, anførte flere medlemsstater imidlertid, at de ikke behandler problemet som en cybersikkerhedstrussel i deres NCSS, men at de derimod håndterer problemet på et bredere samfundsmæssigt plan, f.eks. gennem politiske initiativer.

Sikre banebrydende teknologier (5G, AI, kvantedatabehandling...)

Eftersom det nuværende cybertrusselsbillede gradvist bliver mere omfattende, vil udviklingen af nye teknologier højst sandsynligt resultere i en stigning i intensiteten og antallet af cyberangreb og en diversificering af de metoder, midler og mål, der anvendes af trusselsaktører. Samtidig har disse nye teknologiske løsninger i form af avancerede teknologier potentiale til at blive byggestenene på det europæiske digitale marked. For at beskytte medlemsstaternes stigende digitale afhængighed og fremkomsten af nye teknologier bør der indføres incitamenter og fuldt udbyggede politikker, der skal understøtte en sikker og pålidelig udvikling og udbredelse af disse teknologier i EU.

Under dokumentationsundersøgelsen af medlemsstaternes NCSS'er blev følgende avancerede teknologier fremhævet som relevante for medlemsstaterne: 5G, AI, kvantedatabehandling, kryptografi, edge computing, opkoblede og selvkørende køretøjer, big og smart data, blockchain, robotteknologi og tingenes internet.

I begyndelsen af 2020 offentliggjorde Europa-Kommissionen en meddelelse, hvori den opfordrede medlemsstaterne til at tage skridt til at gennemføre de foranstaltninger, der anbefales i konklusionerne om 5G-værktøjskassen[35]. Denne 5G-værktøjskasse kommer i kølvandet på henstilling (EU) 2019/534 om cybersikkerheden i forbindelse med 5G-net, som Kommissionen vedtog i 2019, og som opfordrede til en fælles europæisk tilgang til sikkerheden i 5G-net[36].

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32019H0534

Under interview, der blev gennemført af ENISA, blev det fremhævet, at dette snarere er et tværgående emne, der behandles i hele NCSS'en, end som et specifikt mål i sig selv.

Sikre datasuverænitet

På den ene side kan cyberspace betragtes som et fantastisk globalt fælles rum, som er let tilgængeligt, giver en høj grad af konnektivitet, og som samtidig kan bane vej for socioøkonomisk vækst. På den anden side er cyberspace også kendetegnet ved en uklar jurisdiktion, vanskeligheder med at tilskrive handlinger, manglende grænser og indbyrdes forbundne net, som kan være skrøbelige, og hvis data kan stjæles eller tilgås af udenlandske regeringer. Ud over disse to perspektiver er det digitale økosystem kendetegnet ved en koncentration af platforme og infrastruktur til onlinetjenester, som er i hænderne på meget få interessenter. Alle ovennævnte aspekter får medlemsstaterne til at fremme digital suverænitet. Digital suverænitet betyder, at borgere og virksomheder er i stand til fuldt ud at udnytte deres potentiale ved at anvende digitale tjenester og IKT-produkter, der er pålidelige og uden at frygte for deres personoplysninger eller digitale aktiver, deres økonomiske autonomi eller politiske indflydelse.

Datasuverænitet eller digital suverænitet fremmes af medlemsstaterne på nationalt plan og på europæisk plan. Det ser ikke ud til, at medlemsstaterne behandler spørgsmålet direkte i deres NCSS som et specifikt mål, men at de enten behandler det som et tværgående princip, eller at de beskriver deres hensigt om at sikre digital suverænitet på nationalt plan i *ad hoc*-publikationer ved at fokusere på centrale teknologier. I Frankrigs strategiske gennemgang af cyberforsvar i 2018 anføres det f.eks., at "kontrol med følgende teknologier er af afgørende betydning for at sikre digital suverænitet: kryptering af kommunikation, detektion af cyberangreb, professionel mobilradio, cloudcomputing og kunstig intelligens"[37].

På europæisk plan deltager medlemsstaterne aktivt i udformningen af den europæiske strategi for data (COM/2020/66 final) og i opbygningen af EU's certificeringsramme for IKT-produkter, -tjenester og -processer, der er fastlagt ved EU's forordning om cybersikkerhed (2019/881) for at sikre strategisk digital autonomi på europæisk plan.

Interviewfasen med medlemsstaterne viste, at spørgsmålet om digital suverænitet ofte betragtes som et mere overordnet spørgsmål end et spørgsmål, der er begrænset til cybersikkerhed. Derfor dækker medlemsstaterne ikke emnet i deres nationale sikkerhedsstrategier, og de få, der gør, dækker det ikke som et specifikt mål i sig selv.

Give incitamenter til udvikling af cyberforsikringsbranchen

Den aktuelle situation i cyberforsikringsbranchen viser, at det globale marked ubestrideligt er vokset. Det er imidlertid stadig i en indledende fase, da der skal indsamles data og registreres mange fortilfælde (f.eks. stiltiende dækning, systemiske cyberrisici osv.). Desuden er de anslåede tab som følge af cyberangreb i hele verden langt højere end den nuværende dækningsgrad i cyberforsikringsbranchen (IMF's arbejdsdokument – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Der er dog afgjort fordele ved at udvikle cyberforsikringsindustrien, og dette kan blive udgangspunktet for positive mekanismer. Cyberforsikringsmekanismer kan specifikt bidrage til:

- Bevidstgørelse af virksomheder om cybersikkerhedsrisici
- Kvantitativ evaluering af eksponeringen for cyberrisici
- Forbedring af styring af cybersikkerhedsrisiko

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

- Støtte til organisationer, der er ofre for cyberangreb
- Dækning af skader (både økonomiske og ikkeøkonomiske) som følge af et cyberangreb.

Nogle medlemsstater har påbegyndt arbejdet med dette emne. F.eks.:

- har Estland i sin NCSS antaget en "vent og se"-tilgang: "For at afbøde cyberrisici i den private sektor i almindelighed vil efterspørgslen efter og udbuddet af cyberforsikringstjenester i Estland blive analyseret, og dette vil danne grundlag for vedtagelsen af samarbejdsprincipper for tilknyttede parter, herunder udveksling af oplysninger, forberedelse af risikovurdering osv. I dag er der kun få udbydere af cyberforsikringstjenester på det estiske marked, og det er nødvendigt først at kortlægge, hvem der tilbyder hvad. Forsikringsbeskyttelsens kompleksitet anses ofte for en hindring for udviklingen af cyberforsikringsmarkedet."
- Luxembourg støtter specifikt udviklingen af cyberforsikringsbranchen i sin NCSS: "Formål 1: Udvikling af nye produkter og tjenester. For at samle risici og tilskynde ofre for digitale cyberhændelser til at søge hjælp fra eksperter til at håndtere hændelsen og genoprette et system, der blev ramt af en ondsindet handling, vil forsikringsselskaber blive tilskyndet til at skabe specifikke produkter til cyberforsikringsområdet."

Der var meget forskellig feedback fra dem, der blev interviewet, om dette emne: Nogle medlemsstater anførte, at man for nylig er begyndt at drøfte cyberforsikringsspørgsmål, mens andre udtalte, at emnet ganske vist er lovende, men at industrien endnu ikke er tilstrækkeligt moden. Et stort antal interviewede erklærede imidlertid, at emnet ikke er behandlet som en del af NCSS, enten fordi det blev anset for at være for specifikt, eller fordi det ikke anses for at være inden for rammerne af NCSS.

TP-02-21-253-DA-N

Om Den Europæiske Unions Agentur for Cybersikkerhed

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, har til formål at bidrage til målsætningen om et højt fælles niveau af cybersikkerhed i Europa. Den Europæiske Unions Agentur for Cybersikkerhed blev oprettet i 2004 og videre styrket ved EU's forordning om cybersikkerhed. Det bidrager til EU's politik for cybersikkerhed, fremmer troværdigheden af IKT-produkter, -tjenester og -processer gennem ordninger for cybersikkerhedscertificering, samarbejder med medlemsstater og EU-organer og ruster Europa til morgendagens cybersikkerhedsudfordringer. Gennem videndeling, kapacitetsopbygning og oplysningskampagner samarbejder agenturet med sine centrale interessenter om at styrke tilliden til den netforbundne økonomi, om at øge EU-infrastrukturens modstandsdygtighed og om i sidste instans at garantere EU's og EU-borgernes digitale sikkerhed. Yderligere oplysninger findes på www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-476-3
DOI: 10.2824/02410