EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CADRUL DE EVALUARE A CAPACITĂȚILOR NAȚIONALE

DECEMBRIE 2020

DESPRE ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică contribuie la politica cibernetică a UE, îmbunătățește fiabilitatea produselor, serviciilor și proceselor TIC prin sistemele de certificare a securității cibernetice, cooperează cu statele membre și cu organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Pentru mai multe informații, consultați www.enisa.europa.eu.

CONTACT

Pentru a lua legătura cu autorii, vă rugăm să utilizați adresa team@enisa.europa.eu.
Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

AUTORI

Anna Sarri, Pinelopi Kyranoudi – Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

MULȚUMIRI

ENISA ar dori să-și exprime aprecierea și recunoștința față de toți experții care au participat și au avut contribuții valoroase la acest raport, în special următorii, în ordine alfabetică:

Biroul central de stat pentru dezvoltarea societății digitale (Croația), Marin Ante Pivcevic

Centrul pentru Securitate Cibernetică (Belgia)

CFCS – Center for Cybersikkerhed (Danemarca), Thomas Wulff

Centrul european de combatere a criminalității informatice – EC3, Alzofra Martinez Alvaro

Centrul european de combatere a criminalității informatice – EC3, Adrian-Ionut Bobeica

Ministerul Federal de Interne (Germania), Sascha-Alexander Lettgen

Administrația pentru securitatea informațiilor (Republica Slovenia), Marjan Kavčič

Guvernul italian (Italia)

Agenția pentru tehnologia informației din Malta (Malta), Katia Bonello și Martin Camilleri

Ministerul Justiției și Securității Publice (Norvegia), Robin Bakke

Ministerul Politicii Digitale (Grecia), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali și Sotiris Vasilos

Ministerul Afacerilor Economice și Comunicațiilor (Estonia), Anna-Liisa Pärnalaas

Agenția națională pentru securitatea cibernetică și a informațiilor (Republica Cehă), Veronika Netolická

Autoritatea Națională de Securitate (Slovacia)

Departamentul de Securitate Națională (Spania), Maria Mar Lopez Gil

NCTV, Ministerul Justiției și Securității (Țările de Jos)

Centrul național portughez de securitate cibernetică (Portugalia), Alexandre Leite și Pedro Matos

Secția de politică de securitate cibernetică, Departamentul pentru mediu, climă și comunicații (Irlanda), James Caffrey

Universitatea Oxford - Global Cyber Security Capacity Centre, Carolin Weisser Harris

De asemenea, ENISA dorește să mulțumească pentru contribuția valoroasă la acest studiu tuturor experților care au furnizat informații, dar care preferă să rămână anonimi.

AVIZ JURIDIC

Trebuie luat în considerare că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu ar trebui interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013.
Această publicație nu reprezintă neapărat stadiul actual al tehnologiei și ENISA o poate actualiza periodic.

Sursele terțe sunt citate în mod corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv al site-urilor externe menționate în această publicație.

Această publicație are doar scop informativ și trebuie să fie accesibilă în mod gratuit. Nici ENISA și nici persoanele care acționează în numele său nu sunt responsabile pentru modul în care ar putea fi utilizate informațiile conținute în această publicație.

AVIZ PRIVIND DREPTURILE DE AUTOR

ISBN: 978-92-9204-491-6

DOI: 10.2824/29660

CATALOG: TP-02-21-253-RO-N

1. CUPRINS

GLOSAR DE TERMENI

ACRONIM	DEFINIȚIE
AAL	Agenție de aplicare a legii
AELS	Asociația Europeană a Liberului Schimb
ARCC	Acord de recunoaștere a criteriilor comune
C&D	Cercetare și dezvoltare
C2M2	Modelul de maturitate a capacității de securitate cibernetică
CCSMM	Modelul comunitar de maturitate în materie de securitate cibernetică
CEC	Cadrul european al calificărilor
CII	Infrastructuri critice de informații
CMM	Modelul de maturitate a capacității de securitate cibernetică pentru națiuni
CMMC	Certificarea modelului de maturitate în materie de securitate cibernetică
CSIRT	Echipe de intervenție în caz de incidente de securitate informatică
CVD	Divulgarea coordonată a vulnerabilității
ECCG	Grupul european pentru certificarea securității cibernetice
ECSM	Luna europeană a securității cibernetice
ECSO	Organizația Europeană de Securitate Cibernetică
GCI	Indicele global de securitate cibernetică
GDS	Serviciu digital guvernamental
IA	Inteligență artificială
IA-CM	Model de măsurare a capacității auditului intern pentru sectorul public
IMM-uri	Întreprinderi mici și mijlocii
IPC	Indicele de putere cibernetică
ISMM	Model de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST
NIS	Securitatea rețelelor și a informațiilor
NIST	Institutul național de standarde și tehnologie
ONL	Ofițeri naționali de legătură
OSE	Operatori de servicii esențiale
OT	Tehnologia de operare

PET	Tehnologii de protecție a vieții private
PIMS	Sistemul de management al informațiilor privind confidențialitatea
PPP	Parteneriate public-privat
PUD	Piața unică digitală
Q-C2M2	Modelul de maturitate a capacității de securitate cibernetică al Qatarului
RGPD	Regulamentul general privind protecția datelor
RPD	Regulamentul privind protecția datelor
SM	Stat membru
SNSC	Strategii naționale de securitate cibernetică
SOG-IS MRA	Grupul de înalți funcționari pentru securitatea sistemelor informatice, acord de recunoaștere reciprocă
TIC	Tehnologia informației și comunicațiilor
UE	Uniunea Europeană
UIT	Uniunea Internațională a Telecomunicațiilor

REZUMAT

Întrucât actualul peisaj al amenințărilor cibernetice continuă să se extindă, iar intensitatea și numărul atacurilor cibernetice continuă să crească, statele membre ale UE trebuie să răspundă în mod eficace prin dezvoltarea și adaptarea în continuare a strategiilor lor naționale de securitate cibernetică (SNSC). De la publicarea primelor studii legate de SNSC de către ENISA în 2012, statele membre ale UE și țările AELS au înregistrat progrese importante în ceea ce privește elaborarea și punerea în aplicare a strategiilor lor.

Prezentul raport prezintă activitatea desfășurată de ENISA în vederea creării unui cadru de evaluare a capacităților naționale (National Capabilities Assessment Framework – NCAF).

Cadrul urmărește să ofere statelor membre o autoevaluare a nivelului lor de maturitate, evaluând obiectivele strategiilor lor naționale de securitate cibernetică, ceea ce le va ajuta să-și sporească și să-și consolideze capacitățile de securitate cibernetică atât la nivel strategic, cât și la nivel operațional.

Acesta prezintă o imagine reprezentativă simplă a nivelului de maturitate în materie de securitate cibernetică al statului membru. NCAF este un instrument care sprijină statele membre:

- să furnizeze informații utile pentru elaborarea unei strategii pe termen lung (de exemplu, bune practici, orientări);
- să contribuie la identificarea elementelor care lipsesc în cadrul SNSC;
- să contribuie la consolidarea în continuare a capacităților de securitate cibernetică;
- să sprijine procesul de responsabilizare a acțiunilor politice;
- să confere credibilitate față de publicul larg și partenerii internaționali;
- să sprijine acțiunile de sensibilizare și îmbunătățire a imaginii publice ca organizație transparentă;
- să ajute la anticiparea problemelor viitoare;
- să ajute la identificarea învățămintelor desprinse și a celor mai bune practici;
- să furnizeze un scenariu de referință privind capacitatea de securitate cibernetică în întreaga UE, pentru a facilita discuțiile și
- să ajute la evaluarea capacităților naționale de securitate cibernetică.

Acest cadru a fost conceput cu sprijinul experților ENISA în domeniu și al reprezentanților din 19 state membre și țări AELS[1]. Publicul-țintă al acestui raport este reprezentat de factori de decizie

[1] Au fost intervievați reprezentanți din următoarele state membre și țări AELS: Belgia, Croația, Republica Cehă, Danemarca, Estonia, Germania, Grecia, Ungaria, Irlanda, Italia, Liechtenstein, Malta, Țările de Jos, Norvegia, Portugalia, Slovacia, Slovenia, Spania, Suedia.

politică, experți și funcționari guvernamentali responsabili sau implicați în conceperea, punerea în aplicare și evaluarea unei SNSC și, la nivel mai larg, a capacităților de securitate cibernetică.

Cadrul de evaluare a capacităților naționale acoperă 17 obiective strategice și este structurat în jurul a patru clustere principale:

- Clusterul #1: Guvernanța și standardele în materie de securitate cibernetică
  1. Elaborarea unui plan național de urgență în domeniul cibernetic
  2. Stabilirea de măsuri de securitate de referință
  3. Asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale

- Clusterul #2: Consolidarea capacităților și acțiuni de sensibilizare
  4. Organizarea de exerciții de securitate cibernetică
  5. Stabilirea unei capacități de reacție la incidente
  6. Sensibilizarea utilizatorilor
  7. Consolidarea programelor de formare și educaționale
  8. Promovarea cercetării și dezvoltării
  9. Oferirea de stimulente pentru ca sectorul privat să investească în măsuri de securitate
  10. Îmbunătățirea securității cibernetice a lanțului de aprovizionare

- Clusterul #3: Aspecte juridice și de reglementare
  11. Protejarea infrastructurilor critice de informații, a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP)
  12. Combaterea criminalității cibernetice
  13. Instituirea unor mecanisme de raportare a incidentelor
  14. Consolidarea protecției vieții private și a datelor

- Clusterul #4: Cooperare
  15. Stabilirea unui parteneriat public-privat
  16. Instituționalizarea cooperării între agenții publice
  17. Implicarea în cooperarea internațională

1. INTRODUCERE

Directiva privind securitatea rețelelor și a informațiilor (NIS), publicată în iulie 2016, impune statelor membre ale UE să adopte o strategie națională privind securitatea rețelelor și a sistemelor informatice, cunoscută și sub denumirea de SNSC (Strategia națională de securitate cibernetică), astfel cum se prevede la articolele 1 și 7. În acest context, o SNSC este definită ca un cadru care stabilește principii strategice, orientări, obiective strategice, priorități, politici și măsuri de reglementare adecvate. Obiectivul preconizat al unei SNSC este de a atinge și a menține un nivel ridicat de securitate a rețelelor și a sistemelor, permițând astfel statelor membre să reducă potențialele amenințări. În plus, SNSC poate reprezenta și un catalizator pentru dezvoltarea industrială și progresul economic și social.

Regulamentul UE privind securitatea cibernetică prevede că ENISA promovează diseminarea celor mai bune practici în definirea și punerea în aplicare a unei SNSC prin sprijinirea statelor membre în adoptarea Directivei NIS și prin colectarea de observații valoroase cu privire la experiențele acestora. În acest scop, ENISA a elaborat mai multe instrumente pentru a sprijini statele membre în elaborarea, punerea în aplicare și evaluarea strategiilor lor naționale de securitate cibernetică (SNSC).

Ca parte a mandatului său, ENISA urmărește să dezvolte un cadru național de autoevaluare a capacităților pentru a măsura nivelul de maturitate al diferitelor SNSC. Obiectivul prezentului raport este de a prezenta studiul realizat în vederea definirii cadrului de autoevaluare.

1.1 SFERA ȘI OBIECTIVELE STUDIULUI

Principalul obiectiv al acestui studiu este de a crea un cadru de autoevaluare a capacităților naționale, denumit ulterior NCAF, pentru a măsura nivelul de maturitate al capacităților de securitate cibernetică ale statelor membre. Mai precis, cadrul trebuie să abiliteze statele membre în ceea ce privește:

- efectuarea evaluării capacităților lor naționale de securitate cibernetică.
- creșterea gradului de sensibilizare cu privire la nivelul de maturitate al țării;
- identificarea domeniilor în care sunt necesare îmbunătățiri și
- consolidarea capacităților de securitate cibernetică.

Acest cadru trebuie să sprijine statele membre, în special factorii de decizie de la nivel național, să efectueze un exercițiu de autoevaluare cu scopul de a îmbunătăți capacitățile naționale de securitate cibernetică.

1.2 ABORDAREA METODOLOGICĂ

Abordarea metodologică utilizată pentru dezvoltarea cadrului de autoevaluare a capacităților naționale se bazează pe patru etape principale:

1. **Cercetare documentară**: Prima etapă a constat în efectuarea unei ample analize a literaturii de specialitate pentru a colecta cele mai bune practici în ceea ce privește elaborarea unui cadru de evaluare a maturității pentru strategiile naționale de securitate cibernetică. Cercetarea documentară se axează pe o analiză sistematică a documentelor relevante privind consolidarea capacităților de securitate cibernetică și definirea strategiei, pe SNSC existente ale statelor membre și pe o comparație a modelelor de maturitate existente în materie de securitate cibernetică. A fost efectuat un exercițiu de evaluare comparativă privind modelele de maturitate existente, prin adoptarea unui cadru de

analiză elaborat în acest scop. Cadrul de analiză se bazează pe metodologia Becker[2] pentru dezvoltarea de modele de maturitate, care stabilește un model de procedură general și consolidat pentru proiectarea de modele de maturitate și prevede cerințe clare pentru dezvoltarea de modele de maturitate. Cadrul de analiză a fost adaptat în continuare pentru a răspunde nevoilor acestui studiu.

2. **Colectarea punctelor de vedere ale experților și ale părților interesate**: Pe baza datelor colectate prin intermediul cercetării documentare și a constatărilor preliminare aferente analizei, această etapă a implicat identificarea și invitarea la interviu a experților identificați care au experiență în elaborarea și punerea în aplicare a unei SNSC sau a unor modele de maturitate. ENISA și-a contactat grupul de experți în strategiile naționale de securitate cibernetică și ofițerii naționali de legătură (ONL) pentru a găsi experții relevanți din fiecare stat membru. În plus, au fost intervievați unii experți implicați în elaborarea modelelor de maturitate. În total, au fost realizate 22 de interviuri, dintre care 19 au fost realizate cu reprezentanți ai agențiilor de securitate cibernetică din diferite state membre (și țări AELS).
3. **Analiza contribuțiilor la bilanț:** Datele culese prin intermediul cercetării documentare și al interviurilor au fost analizate ulterior pentru a identifica cele mai bune practici în elaborarea unui cadru de autoevaluare pentru a măsura maturitatea SNSC, a înțelege nevoile statelor membre și a determina datele care pot fi culese în mod fezabil în diferitele țări europene[3]. Această analiză a permis ajustarea modelului preliminar dezvoltat în etapele anterioare și rafinarea setului de indicatori incluși în model, a nivelurilor de maturitate și a dimensiunilor acestuia.
4. **Finalizarea modelului:** În continuare, o versiune actualizată a cadrului de autoevaluare a capacităților naționale a fost revizuită de experții ENISA în domeniu și a fost validată ulterior de experți prin intermediul unui atelier organizat în octombrie 2020, înainte de publicare.

1.3 PUBLIC-ȚINTĂ

Publicul-țintă al acestui raport este reprezentat de factori de decizie politică, experți și funcționari guvernamentali responsabili sau implicați în conceperea, punerea în aplicare și evaluarea SNSC și, la nivel mai larg, a capacităților de securitate cibernetică. În plus, constatările formalizate în prezentul document pot fi utile experților în materie de politici în materie de securitate cibernetică și cercetătorilor de la nivel național sau european.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application" (Dezvoltarea modelelor de maturitate pentru gestionare IT: un model de procedură și aplicația sa), Business & Information Systems Engineering, vol. 1, nr. 3, pp. 213–222, iunie 2009.
[3] În scopul acestei cercetări, „țările europene" menționate în prezentul raport includ cele 27 de state membre ale UE.

2. CONTEXT

2.1 LUCRĂRI ANTERIOARE PRIVIND CICLUL DE VIAȚĂ AL SNSC

Astfel cum se menționează în Regulamentul UE privind securitatea cibernetică, unul dintre principalele obiective ale ENISA este sprijinirea statelor membre în elaborarea de strategii naționale privind securitatea rețelelor și a sistemelor informatice, promovarea diseminării acestor strategii și monitorizarea punerii lor în aplicare. Ca parte a mandatului său, ENISA a elaborat mai multe documente pe această temă pentru a încuraja schimbul de bune practici și a sprijini punerea în aplicare a SNSC în întreaga UE:

- „Ghidul practic privind etapa de dezvoltare și realizare a SNSC”[4] publicat în 2012
- „Stabilirea cursului pentru eforturile naționale de consolidare a securității în spațiul cibernetic”[5] publicat în 2012
- Primul cadru ENISA de evaluare a SNSC a unui stat membru a fost publicat[6] în 2014.
- „Harta interactivă online a SNSC”[7], publicată în 2014.
- „Ghid de bune practici privind SNSC”[8], publicat în 2016.
- „Instrumentul de evaluare a strategiilor naționale de securitate cibernetică”[9], publicat în 2018.
- „Bunele practici în materie de inovare în domeniul securității cibernetice în cadrul SNSC”[10], document publicat în 2019.

ANEXA A oferă un scurt rezumat al principalelor publicații ale ENISA pe această temă.

Ghidurile și documentele menționate mai sus au fost studiate în cadrul cercetării documentare. În special, „Instrumentul de evaluare a strategiilor naționale de securitate cibernetică”[11] este un

[4] NCSS: Practical Guide on Development and Execution (SNSC: Ghid practic de dezvoltare și realizare) (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 (SNSC: Stabilirea cursului pentru eforturile naționale de consolidare a securității în spațiul cibernetic) (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (Cadrul de evaluare pentru SNSC) (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (Strategiile naționale de securitate cibernetică – hartă interactivă) (ENISA, 2014, actualizată în 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Prezentul document actualizează ghidul din 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Ghidul de bune practici privind SNSC: Conceperea și punerea în aplicare a strategiilor naționale de securitate cibernetică) (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (Instrumentul de evaluare a strategiilor naționale de securitate cibernetică) (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 (Instrumentul de evaluare a strategiilor naționale de securitate cibernetică) (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

element fundamental al NCAF. NCAF se bazează pe obiectivele vizate de instrumentul de evaluare online al SNSC.

2.2 OBIECTIVE COMUNE IDENTIFICATE ÎN CADRUL SNSC EUROPENE

Discrepanța dintre diferitele state membre face dificilă identificarea activităților comune sau a planurilor de acțiune între diferitele contexte naționale, cadre juridice și agende politice. Cu toate acestea, SNSC ale statelor membre au adesea obiective strategice articulate în jurul acelorași subiecte. Astfel, pe baza activității anterioare a ENISA și a analizei SNSC ale statelor membre, au fost identificate 22 de obiective strategice. 15 dintre aceste obiective strategice au fost deja identificate în activitatea anterioară a ENISA, 2 au fost nou adăugate în acest studiu și 5 obiective au fost identificate pentru considerații viitoare.

2.2.1 Obiective strategice comune acoperite de statele membre

Pe baza activității anterioare a ENISA, și anume Instrumentul de evaluare a strategiilor naționale de securitate cibernetică[12], tabelul de mai jos prezintă setul de 15 obiective strategice menționate anterior care sunt abordate în mod curent în cadrul SNSC ale statelor membre. Obiectivele evidențiază nucleul „filozofiei naționale" globale pe această temă. Pentru informații suplimentare cu privire la obiectivele descrise mai jos, vă rugăm să consultați raportul ENISA intitulat „Ghidul de bune practici privind SNSC"[13].

Tabelul 1: Obiective strategice comune acoperite de statele membre în cadrul SNSC

ID	Obiectivele strategice SNSC	Obiective
1	**Elaborarea de planuri naționale de urgență în domeniul cibernetic**	▶ prezentarea și explicarea criteriilor care trebuie utilizate pentru a defini o situație de criză; ▶ definirea proceselor-cheie și a acțiunilor de gestionare a crizei și ▶ definirea clară a rolurilor și responsabilităților diferitelor părți interesate în timpul unei crize cibernetice. ▶ prezentarea și explicarea criteriilor pentru încheierea unei crize și/sau cine are autoritatea de a declara sfârșitul crizei.
2	**Stabilirea de măsuri de securitate de referință**	▶ armonizarea diferitelor practici urmate de organizații atât în sectorul public, cât și în cel privat; ▶ crearea unui limbaj comun între autoritățile publice competente și organizații și deschiderea de canale de comunicare sigure; ▶ facilitarea verificării și evaluării capacităților în materie de securitate cibernetică de către diferitele părți interesate; ▶ schimbul de informații cu privire la bunele practici în materie de securitate cibernetică în fiecare sector industrial și ▶ facilitarea prioritizării investițiilor în materie de securitate de către părțile interesate.
3	**Organizarea de exerciții de securitate cibernetică**	▶ identificarea elementelor care trebuie testate (planuri și procese, persoane, infrastructură, capacități de răspuns, capacități de cooperare, comunicare etc.); ▶ instituirea unei echipe naționale de planificare a exercițiilor cibernetice, cu un mandat clar și ▶ integrarea exercițiilor cibernetice în ciclul de viață al strategiei naționale de securitate cibernetică sau al planului național de urgență în caz de incidente cibernetice.

[12] National Cybersecurity Strategies Evaluation Tool (Instrumentul de evaluare a strategiilor naționale de securitate cibernetică) (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Prezentul document actualizează ghidul din 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Ghidul de bune practici privind SNSC: Conceperea și punerea în aplicare a strategiilor naționale de securitate cibernetică) (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Obiectivele strategice SNSC	Obiective
4	Stabilirea unei capacități de reacție la incidente	▶ mandatul – acesta se referă la competențele, rolurile și responsabilitățile care trebuie atribuite echipei de către guvernul respectiv; ▶ portofoliul de servicii – acesta acoperă serviciile pe care o echipă le furnizează bazei sale de utilizatori sau pe care le utilizează pentru propria funcționare internă; ▶ capacitățile operaționale – acestea se referă la cerințele tehnice și operaționale pe care trebuie să le îndeplinească o echipă și ▶ capacitățile de cooperare – acestea cuprind cerințe privind schimbul de informații cu alte echipe care nu sunt incluse în cele trei categorii anterioare, de exemplu factori de decizie, autorități militare, autorități de reglementare, operatori (infrastructuri critice de informații), autorități de aplicare a legii.
5	Sensibilizarea utilizatorilor	▶ identificarea lacunelor din cunoștințele privind securitatea cibernetică sau aspectele legate de securitatea informațiilor și ▶ eliminarea lacunelor prin acțiuni de sensibilizare sau dezvoltarea/consolidarea bazelor de cunoștințe.
6	Consolidarea programelor de formare și educaționale	▶ consolidarea capacităților operaționale ale forței de muncă existente în domeniul securității informațiilor; ▶ încurajarea studenților să se alăture și ulterior pregătirea acestora pentru a intra în domeniul securității cibernetice; ▶ promovarea și încurajarea relațiilor dintre mediile academice în materie de securitate a informațiilor și industria securității informațiilor și ▶ alinierea formării în materie de securitate cibernetică la nevoile întreprinderilor.
7	Promovarea cercetării și dezvoltării	▶ identificarea cauzelor reale ale vulnerabilităților în loc de remedierea impactului acestora; ▶ reunirea unor oameni de știință din diferite domenii pentru a oferi soluții la probleme multidimensionale și complexe, cum ar fi amenințările fizice și cibernetice; ▶ armonizarea nevoilor industriei cu rezultatele cercetării, facilitând astfel tranziția de la teorie la practică și ▶ identificarea modalităților nu numai de a menține, ci și de a crește nivelul de securitate cibernetică al produselor și serviciilor care sprijină infrastructurile cibernetice existente.
8	Oferirea de stimulente pentru ca sectorul privat să investească în măsuri de securitate	▶ identificarea posibilelor stimulente pentru ca întreprinderile private să investească în măsuri de securitate și ▶ furnizarea de stimulente către întreprinderi pentru a încuraja investițiile în domeniul securității.
9	Protejarea infrastructurilor critice de informații (CII), a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP)	▶ identificarea infrastructurilor critice de informații și ▶ identificarea și atenuarea riscurilor relevante pentru CII.
10	Combaterea criminalității cibernetice	▶ elaborarea de legi în domeniul criminalității informatice și ▶ creșterea eficacității agențiilor de aplicare a legii.
11	Instituirea unor mecanisme de raportare a incidentelor	▶ dobândirea de cunoștințe cu privire la mediul general al amenințărilor; ▶ evaluarea impactului incidentelor (de exemplu, încălcări ale securității, erori de rețea, întreruperi ale serviciului); ▶ dobândirea de cunoștințe cu privire la vulnerabilități și tipuri de atacuri existente și noi; ▶ actualizarea măsurilor de securitate în mod corespunzător și ▶ punerea în aplicare a dispozițiilor Directivei NIS privind raportarea incidentelor.
12	Consolidarea protecției vieții private și a datelor	▶ contribuția la consolidarea drepturilor fundamentale privind viața privată și protecția datelor.
13	Stabilirea unui parteneriat public-privat (PPP)	▶ descurajare (pentru a descuraja atacatorii); ▶ protejare (utilizează cercetarea privind noile amenințări la adresa securității);

ID	Obiectivele strategice SNSC	Obiective
		▶ detectare (utilizează schimbul de informații pentru a face față noilor amenințări); ▶ răspuns (pentru a asigura capacitatea de a face față impactului inițial al unui incident) și ▶ recuperare (pentru a asigura capacitatea de a redresa impactul final al unui incident).
14	Instituționalizarea cooperării între agenții publice	▶ intensificarea cooperării dintre agențiile publice cu responsabilități și competențe legate de securitatea cibernetică; ▶ evitarea suprapunerii competențelor și a resurselor între agențiile publice și ▶ îmbunătățirea și instituționalizarea cooperării dintre agențiile publice în diferite domenii ale securității cibernetice.
15	Implicarea în cooperarea internațională (nu numai cu statele membre ale UE)	▶ beneficierea de crearea unei baze de cunoștințe comune între statele membre ale UE; ▶ crearea de efecte de sinergie între autoritățile naționale competente în domeniul securității cibernetice și ▶ facilitarea și intensificarea luptei împotriva criminalității transnaționale.

2.2.2 Obiective strategice suplimentare

Pe baza cercetărilor documentare efectuate și a interviurilor realizate de ENISA, au fost identificate obiective strategice suplimentare. Statele membre abordează din ce în ce mai mult aceste subiecte în cadrul propriilor SNSC sau definesc planuri de acțiune pe aceeași temă. De asemenea, sunt furnizate exemple de activități puse în aplicare de statele membre. În cazul în care un exemplu provine dintr-o sursă accesibilă publicului, se furnizează o referință. În cazurile în care exemplele se bazează pe interviuri confidențiale cu funcționari din statele membre ale UE, nu sunt furnizate referințe.

Au fost identificate următoarele obiective strategice suplimentare:

- îmbunătățirea securității cibernetice a lanțului de aprovizionare și
- asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale.

Îmbunătățirea securității cibernetice a lanțului de aprovizionare

Întreprinderile mici și mijlocii (IMM-urile) reprezintă coloana vertebrală a economiei europene. Acestea reprezintă 99 % din totalul întreprinderilor din UE[14] și, în 2015, s-a estimat că IMM-urile au creat aproximativ 85 % din locurile de muncă noi și au asigurat două treimi din totalul locurilor de muncă din sectorul privat din UE. În plus, întrucât IMM-urile furnizează servicii întreprinderilor mari și colaborează din ce în ce mai mult cu administrațiile publice[15], trebuie remarcat faptul că, în contextul actual interconectat, IMM-urile constituie legătura slabă pentru atacurile cibernetice. Într-adevăr, IMM-urile sunt cele mai expuse la atacurile cibernetice, însă adesea nu își pot permite să investească în mod adecvat în securitatea cibernetică[16]. Prin urmare, îmbunătățirea securității cibernetice a lanțului de aprovizionare ar trebui să se realizeze cu accent pe IMM-uri.

[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
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

Pe lângă această abordare sistemică, statele membre pot, de asemenea, să pună accentul pe eforturile privind securitatea cibernetică a anumitor servicii și produse TIC care sunt considerate esențiale: tehnologiile TIC utilizate în infrastructurile critice de informații, mecanismele de securitate aplicate în sectorul telecomunicațiilor (controale la nivelul ISP etc.), serviciile de asigurare a încrederii, astfel cum sunt definite în Regulamentul eIDAS și furnizorii de servicii cloud. De exemplu, în strategia sa națională de securitate cibernetică pentru perioada 2019-2024[17], Polonia s-a angajat să dezvolte un sistem național de evaluare și certificare a securității cibernetice ca mecanism de asigurare a calității în lanțul de aprovizionare. Acest sistem de certificare va fi aliniat la cadrul de certificare al UE pentru produsele, serviciile și procesele digitale TIC instituit prin Regulamentul UE privind securitatea cibernetică (2019/881).

Prin urmare, îmbunătățirea securității cibernetice a lanțului de aprovizionare este de o importanță capitală. Acest lucru poate fi realizat, printre altele, prin stabilirea unor politici solide de promovare a IMM-urilor, prin furnizarea de orientări pentru cerințele în materie de securitate cibernetică în cadrul procedurilor de achiziții publice ale administrației publice, prin încurajarea cooperării în sectorul privat, prin crearea de PPP, prin promovarea unor mecanisme de divulgare coordonată a vulnerabilităților (CVD)[18], prin crearea unui sistem de certificare a produselor, inclusiv a componentelor de securitate cibernetică în cadrul inițiativelor digitale pentru IMM-uri, precum și prin finanțarea dezvoltării de competențe.

Asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale

În februarie 2020, Comisia și-a prezentat viziunea pentru transformarea digitală a UE, în comunicarea „Conturarea viitorului digital al Europei”[19], cu scopul de a furniza tehnologii favorabile incluziunii care să funcționeze în favoarea cetățenilor și să respecte valorile fundamentale ale UE. În special, comunicarea afirmă că promovarea transformării digitale a administrațiilor publice în întreaga Europă este esențială. În acest sens, consolidarea încrederii în autoritatea publică în ceea ce privește identitatea digitală și a încrederii în serviciile publice este de o importanță capitală. Acest lucru este cu atât mai important când se ia în considerare faptul că tranzacțiile și schimburile de date din sectorul public au adesea un caracter sensibil.

Multe țări și-au exprimat intenția de a aborda acest subiect în cadrul SNSC, cum ar fi: Danemarca, Estonia, Franța, Luxemburg, Malta, Spania, Țările de Jos și Regatul Unit. Unele dintre aceste țări au afirmat, de asemenea, că acest obiectiv strategic ar putea fi abordat ca parte a unui plan mai amplu:

- Estonia își leagă planul de acțiune asociat privind „Securitatea identității electronice și capacitatea de autentificare electronică” de mai ampla Agendă digitală 2020 pentru Estonia.
- SNSC a Franței indică faptul că secretarul de stat responsabil de tehnologia digitală supraveghează stabilirea unei foi de parcurs „pentru protejarea vieților digitale, a vieții private și a datelor cu caracter personal ale poporului francez”.
- SNSC a Țărilor de Jos menționează că securitatea cibernetică în administrațiile publice, precum și serviciile publice furnizate cetățenilor și întreprinderilor sunt discutate mai în detaliu în Agenda amplă pentru guvernarea digitală.
- Întrucât guvernul Regatului Unit continuă să-și transfere online din ce în ce mai multe servicii, acesta a desemnat Government Digital Service (GDS)(Serviciile digitale guvernamentale) pentru a se asigura că toate noile servicii digitale create sau achiziționate de guvern sunt, de asemenea, „securizate în mod implicit”, cu sprijinul

[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Conturarea viitorului digital al Europei, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

Centrului Național Britanic de Securitate Cibernetică (British National Cybersecurity Centre – NCSC).

2.2.3 Alte obiective strategice avute în vedere

În etapa de cercetare documentară și în cadrul interviurilor realizate de ENISA, au fost studiate și alte obiective strategice. Cu toate acestea, s-a decis că aceste obiective nu vor face parte din cadrul de autoevaluare. ANEXA C – Alte obiective studiate

oferă definiții pentru fiecare dintre obiectivele respective care pot fi utilizate pentru a stimula viitoare discuții cu privire la posibile îmbunătățiri ale SNSC.

Următoarele obiective strategice au fost analizate drept considerații viitoare:

- elaborarea unor strategii sectoriale în materie de securitate cibernetică;
- combaterea campaniilor de dezinformare;
- tehnologii de vârf securizate (5G, IA, informatica cuantică etc.);
- asigurarea suveranității datelor și
- oferirea de stimulente pentru dezvoltarea sectorului asigurărilor cibernetice.

2.3 PRINCIPALELE CONCLUZII ALE EXERCIȚIULUI DE EVALUARE COMPARATIVĂ

Cercetarea documentară cu privire la modelele de maturitate existente legate de securitatea cibernetică a fost efectuată cu scopul de a colecta informații și dovezi în sprijinul elaborării cadrului de autoevaluare a capacităților naționale în domeniul SNSC. În acest context, a fost efectuată o amplă analiză a literaturii de specialitate cu privire la modelele existente pentru a completa constatările cercetării inițiale privind delimitarea domeniului de aplicare a modelelor de maturitate în materie de securitate cibernetică și a SNSC existente, elaborate în secțiunile 2.1 și 2.2. Această revizuire sistematică sprijină selectarea și justificarea nivelurilor de maturitate ale cadrului de evaluare și definirea diferitelor dimensiuni și a diferiților indicatori.

În domeniul de aplicare a revizuirii sistematice a modelelor de maturitate, au fost luate în considerare și analizate 10 modele, pe baza caracteristicilor lor esențiale. Prezentarea generală a caracteristicilor esențiale pentru fiecare model revizuit în cadrul domeniului de aplicare a acestui studiu este disponibilă în Tabelul 2: Prezentare generală a modelelor **de maturitate**, iar o analiză mai detaliată poate fi consultată în ANEXA A.

Tabelul 2: Prezentare generală a modelelor de maturitate

Denumirea modelului	numărul de niveluri de maturitate	numărul de atribute	Metoda de evaluare	Reprezentarea rezultatelor
Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM)	5	5 dimensiuni principale	Colaborarea cu o organizație locală în vederea perfecționării modelului înainte de a-l aplica la contextul național	radar cu 5 secțiuni
Modelul de maturitate a capacității de securitate cibernetică (C2M2)	4	10 domenii principale	Metodologia și setul de instrumente pentru autoevaluare	Tabelul de punctaj cu diagrame
Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice	N/A (4 niveluri)	5 funcții de bază	Autoevaluarea	N/A
Modelul de maturitate a capacității de securitate	5	5 domenii principale	N/A	N/A

cibernetică al Qatarului (Q-C2M2)				
Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)	5	17 domenii principale	Evaluarea de către auditori terți	N/A
Modelul comunitar de maturitate în materie de securitate cibernetică (CCSMM)	5	6 dimensiuni principale	Evaluare în cadrul comunităților cu contribuții din partea agenților de aplicare a legii de stat și federale	N/A
Modelul de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST (ISMM)	5	23 de domenii evaluate	N/A	N/A
Model de măsurare a capacității auditului intern (IA-CM) pentru sectorul public	5	6 elemente	Autoevaluarea	N/A
Indicele global de securitate cibernetică (GCI)	N/A	5 piloni	Autoevaluarea	Tabel de clasificare
Indicele de putere cibernetică (CPI)	N/A	4 categorii	Analiza comparativă realizată de Unitatea de informații a grupului Economist (Economist Intelligence Unit)	Tabel de clasificare

Această revizuire sistematică a permis formularea unor concluzii cu privire la cele mai bune practici adoptate în cadrul modelelor existente pentru a sprijini dezvoltarea modelului conceptual pentru actualul model de maturitate. În special, exercițiul de evaluare comparativă a sprijinit definirea nivelurilor de maturitate, crearea de clustere de dimensiuni și selectarea indicatorilor, precum și o metodologie de vizualizare adecvată pentru rezultatele modelului. Cele mai relevante constatări pentru fiecare dintre aceste elemente sunt detaliate în Tabelul 3.

Tabelul 3: Principalele concluzii ale exercițiului de evaluare comparativă

Caracteristică	Concluzie principală
Niveluri de maturitate	▶ O scară de maturitate pe cinci niveluri pentru cadrele de evaluare a capacităților de securitate cibernetică este în general acceptată și este în măsură să furnizeze rezultate detaliate ale evaluării (vezi Tabelul 6 Comparație între nivelurile de maturitate pentru o imagine exhaustivă a definiției nivelurilor de maturitate pentru fiecare model); ▶ Toate modelele oferă o definiție la nivel înalt a fiecărui nivel de maturitate, care este adaptată ulterior la diferitele dimensiuni sau clustere de dimensiuni; ▶ Când se măsoară maturitatea capabilităților de securitate cibernetică se evaluează, de regulă, două aspecte principale: maturitatea strategiilor și maturitatea proceselor instituite pentru punerea în aplicare a strategiilor.
Atribute	▶ Analiza comparativă a atributelor modelelor de maturitate existente arată rezultate eterogene, cu un număr mediu de atribute per model cuprins între patru și cinci; ▶ Un model care se bazează pe patru sau cinci atribute oferă țărilor nivelul adecvat de granularitate a datelor prin gruparea dimensiunilor relevante și asigurarea lizibilității rezultatelor (a se vedea Tabelul 7: Compararea atributelor/dimensiunilor pentru o descriere a atributelor pentru fiecare model); ▶ Principiul cheie adoptat de toate modelele la definirea clusterelor se bazează pe coerența elementelor grupate în cadrul fiecărui cluster.
Metodă de evaluare	▶ Metodele de evaluare utilizate în diferitele modele analizate variază de la un model la altul; ▶ Cea mai comună metodă de evaluare se bazează pe autoevaluare.
Reprezentarea rezultatelor	▶ Este important să se prezinte rezultatele la diferite niveluri de granularitate; ▶ Metodologia de vizualizare trebuie să fie clară și ușor de citit.

Modelul conceptual s-a bazat pe exercițiul de evaluare comparativă a diferitelor modele de maturitate, precum și pe activitatea anterioară a ENISA. De asemenea, s-a decis să se valorifice *instrumentul interactiv online al ENISA* pentru a elabora indicatori de maturitate utilizați pentru fiecare atribut.

2.4 PROVOCĂRILE EVALUĂRII SNSC

Statele membre se confruntă cu numeroase provocări în consolidarea capacităților de securitate cibernetică, în special când asigură actualizarea capacităților în raport cu cele mai recente evoluții. În continuare este prezentat un rezumat al provocărilor identificate de statele membre și discutate cu acestea în cadrul acestui studiu:

- **Dificultăți în ceea ce privește coordonarea și cooperarea:** coordonarea eforturilor în materie de securitate cibernetică la nivel național pentru a avea un răspuns eficient la problemele de securitate cibernetică se poate dovedi dificilă din cauza numărului mare de părți interesate implicate.
- **Lipsa resurselor pentru efectuarea evaluării:** în funcție de contextul local și de structura de guvernanță națională în materie de securitate cibernetică, evaluarea SNSC și a obiectivelor sale poate dura până la minimum 15 zile de muncă/om.
- **Lipsa sprijinului pentru dezvoltarea capacităților de securitate cibernetică:** Unele state membre au fost de acord că, pentru a susține un buget și a obține sprijin pentru dezvoltarea capacităților de securitate cibernetică, trebuie să parcurgă mai întâi o etapă de evaluare pentru a identifica lacunele și limitările.
- **Dificultăți în ceea ce privește atribuirea succeselor sau modificările strategiei:** Pe măsură ce amenințările evoluează în fiecare zi și tehnologia se îmbunătățește, planurile de acțiune trebuie să fie permanent adaptate ca răspuns. Cu toate acestea, evaluarea unei SNSC și atribuirea modificărilor strategiei în sine rămâne o sarcină dificilă. Acest lucru, la rândul său, face dificilă identificarea limitărilor și a deficiențelor SNSC.

- **Dificultăți în evaluarea eficacității SNSC:** Se pot colecta indicatori pentru a evalua diferite domenii, cum ar fi progresele înregistrate, punerea în aplicare, maturitatea și eficacitatea. Deși măsurarea progreselor și a punerii în aplicare este relativ ușoară în comparație cu măsurarea eficacității, aceasta din urmă rămâne mai semnificativă pentru evaluarea rezultatelor și a impactului unui SNSC. Pe baza interviurilor realizate de ENISA, un număr mare de state membre au declarat că măsurarea cantitativă a eficacității unei SNSC este importantă, dar reprezintă, de asemenea, o sarcină foarte solicitantă, care este destul de dificilă în unele cazuri.
- **Dificultatea adoptării unui cadru comun:** Statele membre ale UE își desfășoară activitatea în diferite contexte în ceea ce privește politica, organizațiile, cultura, structura societății și maturitatea SNSC. Anumite state membre intervievate în cadrul acestui studiu au afirmat că ar putea fi dificil să susțină și să utilizeze un cadru de autoevaluare universal.

2.5 BENEFICIILE UNEI EVALUĂRI A CAPACITĂȚILOR NAȚIONALE

Începând din 2017, toate statele membre ale UE au o SNSC[20]. Deși acest lucru reprezintă o evoluție pozitivă, este important, de asemenea, ca statele membre să fie în măsură să evalueze în mod corespunzător aceste SNSC, aducând astfel valoare adăugată planificării strategice și punerii în aplicare a acestora.

Unul dintre obiectivele cadrului de evaluare a capacităților naționale este de a evalua capacitățile de securitate cibernetică pe baza priorităților stabilite în diferitele SNSC. În mod fundamental, cadrul evaluează nivelul de maturitate al capacităților de securitate cibernetică ale statelor membre în domeniile definite de obiectivele SNSC. Astfel, rezultatele cadrului sprijină factorii de decizie din statele membre în definirea strategiei naționale privind securitatea cibernetică, oferindu-le informații naționale cu privire la situația actuală[21]. În cele din urmă, NCAF este menit să ajute statele membre să identifice domeniile de îmbunătățire și de consolidare a capacităților.

Cadrul urmărește să ofere statelor membre o autoevaluare a nivelului lor de maturitate, evaluând obiectivele strategiilor lor naționale de securitate cibernetică, ceea ce le va sprijini să-și sporească și să-și consolideze capacitățile de securitate cibernetică atât la nivel strategic, cât și la nivel operațional.

Într-o abordare mai practică, pe baza interviurilor realizate de ENISA cu mai multe agenții responsabile de domeniul securității cibernetice în diferite state membre, au fost identificate și subliniate următoarele beneficii ale cadrului de evaluare a capacităților naționale:

- să furnizeze informații utile pentru elaborarea unei strategii pe termen lung (de exemplu, bune practici, orientări);
- să contribuie la identificarea elementelor lipsă în cadrul SNSC;
- să contribuie la consolidarea în continuare a capacităților de securitate cibernetică;
- să sprijine procesul de responsabilizare a acțiunilor politice;
- să confere credibilitate față de publicul larg și față de partenerii internaționali;
- să sprijine acțiunile de sensibilizare și îmbunătățire a imaginii publice ca organizație transparentă;
- să ajute la anticiparea problemelor viitoare;
- să ajute la identificarea învățămintelor desprinse și a celor mai bune practici;

[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 (Interfața dintre evaluare și ordinea publică. Evaluare), 5(4), 468-486.

- să furnizeze un scenariu de referință privind capacitatea de securitate cibernetică în întreaga UE, pentru a facilita discuțiile și
- să ajute la evaluarea capacităților naționale de securitate cibernetică.

3. METODOLOGIA CADRULUI DE EVALUARE A CAPACITĂȚILOR NAȚIONALE

3.1 OBIECTIVUL GENERAL

Principalul obiectiv al NCAF este de a măsura nivelul de maturitate al capacităților de securitate cibernetică ale **statelor membre** pentru a le sprijini în efectuarea unei evaluări a capacității lor naționale de securitate cibernetică, în sporirea gradului de sensibilizare cu privire la nivelul de maturitate a țării, în identificarea domeniilor în care se pot aduce îmbunătățiri și în consolidarea capacităților de securitate cibernetică.

3.2 NIVELURI DE MATURITATE

Cadrul se bazează pe **cinci niveluri de maturitate** care definesc etapele parcurse de statele membre atunci când consolidează capacități de securitate cibernetică în domeniul acoperit de fiecare obiectiv al SNSC. Nivelurile reprezintă niveluri de maturitate în creștere, pornind de la **nivelul 1** inițial, în care statele membre nu au o abordare clar definită pentru consolidarea capacităților de securitate cibernetică în domeniile vizate de obiectivele SNSC și terminând cu **nivelul 5**, în care strategia de consolidare a capacităților de securitate cibernetică este dinamică și adaptabilă la evoluțiile mediului. Tabelul 4 prezintă scara nivelurilor de maturitate, cu o descriere a fiecărui nivel de maturitate.

Tabelul 4: Grila de maturitate pe cinci niveluri a Cadrului ENISA de evaluare a capacităților naționale

NIVELUL 1 – INIȚIAL/AD-HOC	NIVELUL 2 – DEFINIȚIE TIMPURIE	NIVELUL 3 – STABILIRE	NIVELUL 4 – OPTIMIZARE	NIVELUL 5 – ADAPTABILITATE
Statul membru nu are o abordare clar definită pentru consolidarea capacităților de securitate cibernetică în domeniile vizate de obiectivele SNSC. Cu toate acestea, este posibil ca țara să aibă anumite obiective generice și să fi realizat unele studii (tehnice, politice, de politică) pentru a îmbunătăți capacitățile naționale.	A fost definită abordarea națională pentru consolidarea capacităților în domeniul vizat de obiectivele SNSC. Planurile de acțiune sau activitățile pentru obținerea rezultatelor sunt instituite, dar se află într-un stadiu incipient. În plus, este posibil să fi fost identificate și/sau implicate părți interesate active.	Planul de acțiune pentru consolidarea capacităților în domeniul vizat de obiectivele SNSC este clar definit și sprijinit de părțile interesate relevante. Practicile și activitățile sunt puse în aplicare în mod uniform la nivel național. Activitățile sunt definite și documentate cu o alocare clară a resurselor și o guvernanță clară, precum și un set de termene.	Planul de acțiune este evaluat în mod regulat: acesta este prioritizat, optimizat și durabil. Performanța activităților de consolidare a capacităților de securitate cibernetică este evaluată periodic. Se identifică factorii de succes, provocările și lacunele în punerea în aplicare a activităților.	Strategia de consolidare a capacităților de securitate cibernetică este dinamică și adaptativă. Atenția constantă acordată evoluțiilor de mediu (progrese tehnologice, conflicte globale, noi amenințări etc.) favorizează o capacitate de decizie rapidă și capacitatea de a acționa rapid în vederea îmbunătățirii.

3.3 CLUSTERELE ȘI STRUCTURA GENERALĂ A CADRULUI DE AUTOEVALUARE

Cadrul de autoevaluare este caracterizat prin **patru clustere**: (I) Guvernanța și standardele în materie de securitate cibernetică, (II) Consolidarea capacităților și acțiuni de sensibilizare, (III) Aspectele juridice și de reglementare și (IV) Cooperarea. Fiecare dintre aceste clustere acoperă un domeniu tematic cheie pentru consolidarea capacităților de securitate cibernetică într-o țară și conține un ansamblu de obiective diferite pe care statele membre l-ar putea include în propriile SNSC. În special:

- **(I) Guvernanța și standardele în materie de securitate cibernetică**: acest cluster măsoară capacitatea statelor membre de a institui o guvernanță, standarde și bune practici adecvate în domeniul securității cibernetice. Această dimensiune ia în considerare diferite aspecte ale apărării și rezilienței cibernetice, sprijinind, în același timp, dezvoltarea industriei naționale a securității cibernetice și consolidând încrederea în guverne;
- **(II) Consolidarea capacităților și acțiuni de sensibilizare**: acest cluster evaluează capacitatea statelor membre de a sensibiliza publicul cu privire la riscurile și amenințările în materie de securitate cibernetică și la modul de abordare a acestora. În plus, această dimensiune măsoară capacitatea țării de a consolida în permanență capacitățile în materie de securitate cibernetică și de a spori nivelul general de cunoștințe și competențe în acest domeniu. Aceasta abordează dezvoltarea pieței securității cibernetice și progresele în domeniul C&D în materie de securitate cibernetică**.** Acest cluster regrupează toate obiectivele care stau la baza consolidării capacităților;
- **(III) Aspectele juridice și de reglementare**: acest cluster măsoară capacitatea statelor membre de a institui instrumentele juridice și de reglementare necesare pentru a aborda și a contracara creșterea criminalității informatice și a incidentelor cibernetice conexe, precum și pentru a proteja infrastructurile critice de informații. În plus, această dimensiune evaluează, de asemenea, capacitatea statelor membre de a crea un cadru juridic pentru a proteja cetățenii și întreprinderile, de exemplu în cazul unui echilibru între securitate și viața privată și
- **(IV) Cooperarea:** acest cluster evaluează cooperarea și schimbul de informații între diferite grupuri de părți interesate la nivel național și internațional ca fiind un instrument important pentru o mai bună înțelegere și reacție la un mediu al amenințărilor aflat în continuă schimbare.

Obiectivele care au fost incluse în model sunt cele care sunt adoptate în comun de statele membre și au fost selectate dintre obiectivele enumerate în secțiunea 2.2. În special, modelul evaluează următoarele obiective:

- 1. elaborarea de planuri naționale de urgență în domeniul cibernetic (I)
- 2. stabilirea de măsuri de securitate de referință (I)
- 3. asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale (I)
- 4. stabilirea unei capacități de reacție la incidente (II)
- 5. sensibilizarea utilizatorilor (II)
- 6. organizarea de exerciții de securitate cibernetică (II)
- 7. consolidarea programelor de formare și educaționale (II)
- 8. promovarea cercetării și dezvoltării (C&D)
- 9. oferirea de stimulente pentru ca sectorul privat să investească în măsuri de securitate (II)
- 10. îmbunătățirea securității cibernetice a lanțului de aprovizionare (II)
- 11. protejarea infrastructurilor critice de informații, a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP) (III)
- 12. combaterea criminalității cibernetice (III)
- 13. instituirea unor mecanisme de raportare a incidentelor (III)
- 14. consolidarea protecției vieții private și a datelor (III)
- 15. instituționalizarea cooperării între agenții publice (IV)
- 16. implicarea în cooperarea internațională (IV)
- 17. stabilirea unui parteneriat public-privat (IV)

Cele patru clustere și obiectivele subiacente sunt combinate în cadrul modelului pentru a avea o perspectivă holistică asupra maturității capacităților de securitate cibernetică ale statelor membre. Figura 1 prezintă structura generală a cadrului de autoevaluare și arată modul în care aceste elemente, și anume obiectivele, clusterele și cadrul de autoevaluare, sunt legate de evaluarea performanței unei țări.

Figura 1: Structura cadrului de autoevaluare

Pentru fiecare obiectiv inclus în cadrul de autoevaluare, există o serie de indicatori distribuiți între cele cinci niveluri de maturitate. Fiecare indicator se bazează pe o întrebare dihotomică (da/nu). Indicatorul poate fi obligatoriu sau neobligatoriu.

3.4 MECANISMUL DE PUNCTARE

Mecanismul de punctare al cadrului de autoevaluare ia în considerare elementele menționate mai sus și principiile enumerate în secțiunea 3.5. În fapt, modelul oferă un punctaj bazat pe valoarea a doi parametri, **nivelul de maturitate** și **rata de acoperire**. Fiecare dintre acești parametri poate fi calculat la diferite niveluri: (i) pe obiectiv, (ii) pe cluster de obiective sau (iii) global.

Punctaje la nivel de obiectiv

Punctajul pentru nivelul de maturitate oferă o imagine de ansamblu asupra nivelului de maturitate, arătând ce capacități și practici au fost puse în aplicare. Punctajul pentru nivelul de maturitate este calculat ca fiind cel mai înalt nivel pentru care respondentul a îndeplinit toate condițiile necesare (și anume, răspunsul este DA la toate întrebările obligatorii), pe lângă faptul că a îndeplinit toate condițiile pentru nivelurile anterioare de maturitate.

Rata de acoperire arată gradul de acoperire al tuturor indicatorilor pentru care răspunsul este pozitiv, indiferent de nivelul lor. Aceasta este o valoare complementară care ia în considerare toți indicatorii care măsoară un obiectiv. Rata de acoperire este calculată ca raportul dintre numărul total de întrebări din cadrul obiectivului și numărul de întrebări la care răspunsul este pozitiv.

Este important să se clarifice faptul că, în restul documentului, cuvântul ***punctaj*** este utilizat pentru a face referire atât la valorile nivelului de maturitate, cât și la rata de acoperire.

Figura 2 – Mecanismul de punctare pentru fiecare obiectiv oferă o vizualizare a mecanismului de evaluare descris în secțiunea 3.1 care va fi dezvoltată mai jos.

Figura 2: Mecanismul de punctare pentru fiecare obiectiv

Figura 2 prezintă un exemplu pentru modul în care nivelul de maturitate este calculat în funcție de obiectiv. Trebuie remarcat faptul că respondentul a îndeplinit toate condițiile primelor trei niveluri de maturitate și le-a îndeplinit doar parțial pe cele de nivel 4. Prin urmare, punctajul indică faptul că ***nivelul de maturitate al respondentului este nivelul 3 pentru obiectivul „Organizarea exercițiului de securitate cibernetică”*** *.*

Cu toate acestea, în exemplul descris în Figura 2, nivelul de maturitate al obiectivului nu este în măsură să surprindă informațiile furnizate de indicatorii care au un scor pozitiv și care depășesc nivelul 3 de maturitate. În acest caz, rata de acoperire poate oferi o imagine de ansamblu asupra tuturor elementelor pe care respondentul le-a pus în aplicare pentru a atinge obiectivul respectiv, în pofida nivelului său real de maturitate. În acest caz, proporția dintre numărul total de întrebări din cadrul obiectivului și numărul de întrebări pentru care răspunsul este pozitiv este egal cu 19/27, și anume ***valoarea ratei de acoperire este de 70 %.***

În plus, pentru a se adapta la particularitățile statelor membre, permițând totodată o imagine de ansamblu coerentă, punctajul este calculat pe baza a două eșantioane diferite la nivel de cluster și la nivel global:

- **Punctaje generale:** un eșantion complet care acoperă toate obiectivele incluse în cluster sau în cadrul global (de la unu la 17);
- **Punctaje specifice:** un eșantion specific care acoperă numai obiectivele selectate de statul membru (care corespund, de regulă, obiectivelor prezente în SNSC a țării respective) în cluster sau în cadrul global.

Punctaje la nivel de cluster

Nivelul general de maturitate al fiecărui cluster se calculează ca media aritmetică a nivelului de maturitate al tuturor obiectivelor din cadrul clusterului respectiv.

Nivelul specific de maturitate al fiecărui cluster se calculează ca media aritmetică a nivelului de maturitate a obiectivelor din cadrul clusterului pe care statul membru a ales să îl evalueze (corespunzând de fapt obiectivelor prezente în SNSC a țării respective).

De exemplu, Figura 1 arată că în clusterul (I) Guvernanța și standardele în materie de securitate cibernetică sunt cuprinse trei obiective. Presupunând că respondentul a ales să evalueze numai primele două obiective, dar nu și cel de al treilea, și presupunând că primele două obiective prezintă un nivel de maturitate 2 și, respectiv, 4, atunci nivelul de maturitate al clusterului, luând în considerare toate obiectivele, este nivelul 2 [nivelul generic de maturitate al clusterului (I) = (2+4)/3], în timp ce nivelul de maturitate al clusterului luând în considerare numai obiectivele specifice selectate de evaluator este nivelul 3 [nivelul specific de maturitate al clusterului (I) = (2+4)/2].

Rata de acoperire generală a fiecărui cluster se calculează ca proporție între numărul total de întrebări din cadrul clusterului și numărul de întrebări la care răspunsul este pozitiv.

Rata de acoperire specifică a fiecărui cluster se calculează ca fiind proporția dintre numărul total de întrebări din cadrul clusterului referitoare la obiectivele pe care statul membru a ales să le evalueze (care corespund, de regulă, obiectivelor existente în SNSC a țării respective) și numărul de întrebări la care răspunsul este pozitiv.

Punctaje la nivel global

Nivelul general global de maturitate al unei țări se calculează ca medie aritmetică a nivelului de maturitate al tuturor obiectivelor incluse în cadru, de la 1 la 17.

Nivelul specific global de maturitate al unei țări se calculează ca medie aritmetică a nivelului de maturitate a obiectivelor incluse în cadru pe care statul membru a ales să îl evalueze (corespunzând, de regulă, obiectivelor prezente în SNSC a țării respective).

Rata de acoperire generală globală a unei țări se calculează ca raport dintre numărul total de întrebări din toate obiectivele incluse în cadru (de la 1 la 17) și numărul de întrebări la care răspunsul este pozitiv.

Rata de acoperire specifică globală a unei țări se calculează ca raport dintre numărul total de întrebări din obiectivele incluse în cadru pe care statul membru a ales să le evalueze (corespunzând, de regulă, obiectivelor existente în SNSC a țării respective) și numărul de întrebări la care răspunsul este pozitiv.

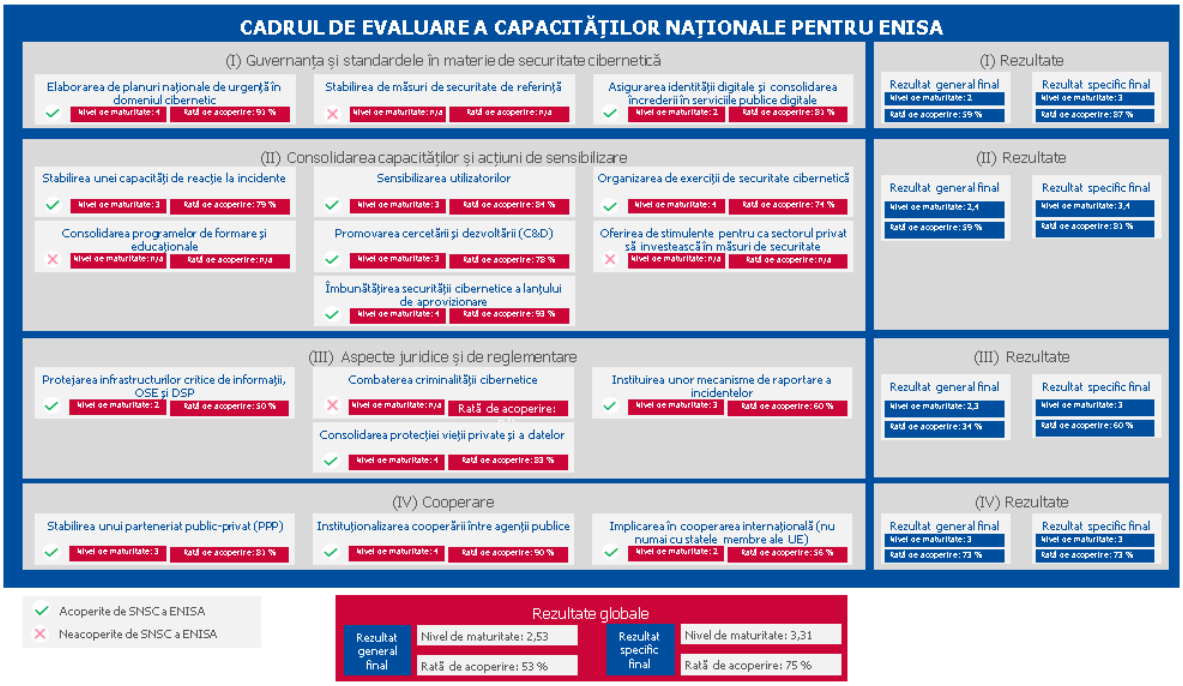
Pentru fiecare indicator, respondenții pot selecta o a treia opțiune „nu știu/nu se aplică” pentru răspunsul lor. În acest caz, indicatorul este exclus din calculul total al rezultatelor.

Nivelurile de maturitate la nivel de cluster și la nivel global sunt calculate cu o medie aritmetică pentru a arăta progresele înregistrate între două evaluări. Într-adevăr, alternativa care constă în calcularea nivelurilor de maturitate al clusterului și global ca nivel de maturitate al obiectivului cel mai puțin matur – deși relevantă din punct de vedere al maturității – nu poate ține seama de progresele înregistrate în domenii acoperite de alte obiective.

Întrucât nivelul de cluster și nivelul global sunt consolidate în scopul raportării, s-a optat pentru utilizarea mediei aritmetice. Pentru o mai mare acuratețe, vă rugăm să utilizați punctajele la nivel de obiectiv în scopul raportării.

Figura 3 de mai jos sintetizează mecanismele de punctare de la diferite niveluri ale modelului (obiectiv, cluster, global).

Figura 3: Mecanismul general de punctare



3.5 CERINȚE PENTRU CADRUL DE AUTOEVALUARE

Cadrul de evaluare a capacităților naționale prezentat în această secțiune se bazează pe nevoile evidențiate de statele membre și este construit în jurul unui set de cerințe enumerate în continuare:

- NCAF este utilizat în mod voluntar de către statul membru ca un cadru de autoevaluare;
- NCAF vizează măsurarea capacităților de securitate cibernetică ale statelor membre în ceea ce privește cele 17 obiective. Cu toate acestea, statul membru poate să aleagă obiectivele în raport cu care dorește să efectueze evaluarea și să evalueze doar un subset din cele 17 obiective;
- cadrul de autoevaluare vizează măsurarea nivelului de maturitate al capacităților de securitate cibernetică ale statului membru;
- rezultatele evaluării nu sunt publicate decât dacă statul membru decide să facă acest lucru din proprie inițiativă;
- statul membru poate afișa rezultatele evaluării prin prezentarea nivelului de maturitate a capacităților țării în materie de securitate cibernetică, a unui cluster de obiective sau chiar a unui singur obiectiv;
- toate obiectivele evaluate sunt la fel de relevante în cadrul de evaluare și, prin urmare, au aceeași importanță. Același lucru este valabil pentru indicatorii introduși în cadrul său și
- statul membru este în măsură să își monitorizeze progresele în timp.

Cadrul de autoevaluare are ca scop sprijinirea statelor membre în ceea ce privește consolidarea capacităților de securitate cibernetică deoarece include, de asemenea, un set de

recomandări sau orientări care să ghideze țările europene în vederea îmbunătățirii nivelului lor de maturitate.

Notă: aceste recomandări sau orientări sunt generice și se bazează pe publicațiile ENISA și pe lecțiile învățate din alte țări și vor ține cont de rezultatul autoevaluării.

4. INDICATORII NCAF

4.1 INDICATORII CADRULUI

Această secțiune prezintă indicatorii Cadrului ENISA de evaluare a capacităților naționale. Următoarele secțiuni sunt organizate pe clustere.

Pentru fiecare cluster, un tabel prezintă setul cuprinzător de indicatori sub formă de întrebări reprezentative pentru un anumit nivel de maturitate. Chestionarul este principalul instrument de autoevaluare. Pentru fiecare obiectiv, trebuie să se noteze două seturi de indicatori:

- un set de întrebări generice privind maturitatea strategiei (9 întrebări generice), marcate de la „a” la „c” pentru fiecare nivel de maturitate, repetate pentru fiecare obiectiv și
- un set de întrebări privind capacitatea de securitate cibernetică (319 întrebări privind capacitatea de securitate cibernetică), numerotate de la „1” la „10” pentru fiecare nivel de maturitate, specifice domeniului vizat de obiectiv.

Fiecare întrebare este însoțită de o etichetă (0-1) care indică dacă întrebarea este un indicator obligatoriu (1) sau un indicator neobligatoriu (0) pentru nivelul de maturitate.

Fiecare întrebare poate fi identificată printr-un număr de identificare format din:

- numărul obiectivului;
- nivelul de maturitate și
- numărul întrebării.

De exemplu, întrebarea ID 1.2.4 este a patra întrebare de la nivelul de maturitate 2 al obiectivului strategic (I) „Elaborarea de planuri naționale de urgență în domeniul cibernetic”.

Trebuie remarcat faptul că, în tot cuprinsul chestionarului, domeniul de aplicare a întrebărilor este la nivel național, cu excepția cazului în care se prevede altfel. În toate întrebările, pronumele „dumneavoastră” se referă în mod generic la statul membru și nu se referă la persoana sau organismul guvernamental care efectuează evaluarea.

Definiția fiecărui obiectiv poate fi consultată în capitolul 2.2 - Obiective comune identificate în cadrul SNSC europene.

4.1.1 Clusterul #1: Guvernanța și standardele în materie de securitate cibernetică

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
1 – Elaborarea de planuri naționale de urgență în domeniul cibernetic	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să-l includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați început să lucrați la elaborarea unor planuri naționale de urgență în domeniul cibernetic? (de exemplu, stabilirea obiectivelor generale, a domeniului de aplicare și/sau a principiilor planurilor de urgență etc.)	1	Aveți o doctrină/o strategie națională care include securitatea cibernetică ca factor de criză (de exemplu, un plan, o politică etc.)?	1	Aveți un plan de gestionare a crizelor cibernetice la nivel național?	1	Sunteți mulțumit de numărul sau procentajul sectoarelor critice incluse în planul național de intervenție în domeniul cibernetic?	1	Aveți un proces de desprindere de învățăminte în urma exercițiilor cibernetice sau a crizelor efective la nivel național?	1
	2	Este înțeles, în general, că incidentele cibernetice constituie un factor de criză care ar putea amenința securitatea națională?	0	Dispuneți de un centru pentru a obține informații și pentru a informa factorii de decizie? Și anume, orice metode, platforme sau locații pentru a se asigura că toți actorii implicați în gestionarea situațiilor de criză pot avea acces la aceleași informații în timp real cu privire la criza cibernetică.	1	Dispuneți de proceduri specifice crizei cibernetice la nivel național?	1	Organizați activități (de exemplu, exerciții) legate de planificarea națională pentru situații de urgență în domeniul cibernetic suficient de frecvent?	1	Dispuneți de un proces de testare periodică a planului național?	1
	3	Au fost efectuate studii (tehnice, operaționale, politice) în domeniul planificării pentru situații de urgență în domeniul cibernetic?	0	Sunt angajate resursele relevante pentru a supraveghea elaborarea și realizarea planurilor naționale de urgență în domeniul cibernetic?	1	Dispuneți de o echipă de comunicare special formată pentru a răspunde la crizele cibernetice și pentru a informa publicul?	1	Aveți suficiente persoane dedicate planificării crizelor, analizării învățămintelor desprinse și punerii în aplicare a modificărilor?	1	Dispuneți de instrumente și platforme adecvate pentru a consolida conștientizarea situației?	1
	4	-		Dispuneți de o metodologie de evaluare a amenințărilor cibernetice la nivel național care include proceduri pentru evaluarea impactului?	0	Implicați toate părțile interesate relevante de la nivel național (securitatea națională, apărarea, protecția civilă, aplicarea legii, ministerele, autoritățile etc.)?	1	Dispuneți de suficiente persoane instruite pentru a răspunde la crize cibernetice la nivel național?	1	Urmați un model specific de maturitate pentru a monitoriza și a îmbunătăți planul de urgență în domeniul cibernetic?	0

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	5	-		-		Dispuneți de instalații adecvate de gestionare a crizelor și de celule de supraveghere?	1	-		Dispuneți de resurse specializate în anticiparea amenințărilor sau lucrați la o viitoare securitate cibernetică pentru a face față viitoarelor crize sau provocărilor de mâine?	0
	6	-		-		Intrați în dialog cu părțile interesate internaționale din UE, dacă este necesar?	0	-		-	
	7	-		-		Intrați în dialog cu părți interesate internaționale din țări din afara UE, dacă este necesar?	0	-		-	
2 – Stabilirea de măsuri de securitate de referință	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați efectuat un studiu pentru a identifica cerințele și lacunele pentru organizațiile **publice** pe baza standardelor recunoscute la nivel internațional? (de exemplu, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS etc.)	1	Sunt conforme măsurile de securitate stabilite cu standardele internaționale/naționale?	1	Sunt obligatorii măsurile de securitate de referință?	1	Există un proces de actualizare frecventă a măsurilor de securitate de referință?	1	Dispuneți de un proces de întărire a TIC în cazul în care incidentele nu sunt abordate de măsuri?	1
	2	Ați efectuat un studiu pentru a identifica cerințele și lacunele pentru organizațiile **private** pe baza standardelor recunoscute la nivel internațional? (de exemplu, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS etc.)	1	Se consultă sectorul privat și alte părți interesate atunci când se definesc măsurile de securitate de referință?	1	Puneți în aplicare măsuri de securitate orizontale în sectoarele critice?	1	Există un mecanism de monitorizare pentru a examina adoptarea măsurilor de securitate de referință?	1	Evaluați relevanța noilor standarde care sunt elaborate ca răspuns la cele mai recente evoluții din peisajul amenințărilor?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	3	-		-		Puneți în aplicare măsuri de securitate sectoriale specifice în sectoarele critice?	1	Există o autoritate națională care să verifice dacă măsurile de securitate de referință sunt aplicate sau nu?	1	Utilizați sau promovați un proces național de divulgare coordonată a vulnerabilităților (CVD)?	1
	4	-				Sunt măsurile de securitate de referință conforme cu sistemele de certificare relevante?	1	Dispuneți de un proces de identificare a organizațiilor neconforme într-o anumită perioadă de timp?	1	-	
	5	-		-		Există un proces de autoevaluare a riscurilor pentru măsurile de securitate de referință?	1	Există un proces de audit pentru a se asigura că măsurile de securitate sunt aplicate în mod corespunzător?	1	-	
2 – Stabilirea de măsuri de securitate de referință	6	-		-		Revizuiți măsurile de securitate de referință obligatorii în procesul de achiziții publice al organismelor guvernamentale?	0	Definiți sau încurajați în mod activ adoptarea unor standarde sigure pentru dezvoltarea de produse IT/OT esențiale (echipamente medicale, vehicule conectate și autonome, echipamente radio profesionale, echipamente industriale grele etc.)?	0	-	
3 – Asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați efectuat studii sau analize ale lacunelor pentru a identifica nevoile de a asigura servicii publice digitale pentru cetățeni și întreprinderi?	1	Efectuați analize de risc pentru a determina profilul de risc al activelor sau serviciilor înainte de a le transfera în cloud sau pentru a se angaja în proiecte de transformare digitală?	1	Promovați metodologii de protecție a vieții private începând cu momentul conceperii în toate proiectele de e-guvernare?	1	Colectați indicatori privind incidentele de securitate cibernetică care implică încălcarea serviciilor publice digitale?	1	Participați la grupuri de lucru europene pentru a menține standardele și/sau pentru a elabora noi cerințe pentru serviciile electronice de asigurare a încrederii (semnături electronice, sigilii electronice, servicii de distribuție electronică înregistrată, marcare temporală, autentificarea unui site internet)? (de exemplu ETSI/CEN/CENELEC, ISO, IETF, NIST, UIT etc.)	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
3 – Asigurarea identității digitale și consolidarea încrederii în serviciile publice digitale	2	-		Dispuneți de o strategie de creare sau promovare a unor sisteme naționale sigure de identificare electronică (eID) pentru cetățeni și întreprinderi?	1	Includeți părți interesate din sectorul privat în conceperea și furnizarea de servicii publice digitale sigure?	1	Ați pus în aplicare recunoașterea reciprocă a mijloacelor de identificare electronică cu alte state membre?	1	Participați activ la evaluările inter pares ca parte a notificării Comisiei Europene cu privire la sistemele de identificare electronică?	1
	3	-		Aveți o strategie pentru dezvoltarea sau promovarea de servicii de încredere pentru tranzacții electronice naționale sigure (semnături electronice, sigilii electronice, servicii de distribuție electronică înregistrată, marcare temporală, autentificarea unui site internet) pentru cetățeni și întreprinderi?	1	Puneți în aplicare un nivel minim de securitate de bază pentru toate serviciile publice digitale?	1	-		-	
	4	-		Aveți o strategie privind cloud-ul guvernamental (o strategie de cloud computing orientată către guvern și organisme publice precum ministerele, agențiile guvernamentale și administrațiile publice etc.) care ia în considerare implicațiile pentru securitate?	0	Sunt disponibile sisteme de identificare electronică pentru cetățeni și întreprinderi cu un nivel de asigurare substanțial sau ridicat, astfel cum sunt definite în anexa la Regulamentul (UE) nr. 910/2014 privind e-IDAS?	1	-		-	
	5	-		-		Dispuneți de servicii publice digitale care necesită sisteme de identificare electronică cu un nivel de asigurare substanțial sau ridicat, astfel cum sunt definite în anexa la Regulamentul (UE) nr. 910/2014 privind e-IDAS?	1	-		-	
	6	-		-		Aveți furnizori de servicii de încredere pentru cetățeni și întreprinderi (semnături electronice, sigilii electronice, servicii de distribuție electronică înregistrată, marcare temporală, autentificarea unui site internet)?	1	-		-	
	7	-		-		Promovați adoptarea unor măsuri de securitate de bază pentru toate modelele de implementare a cloud-ului (de exemplu, IaaS, PaaS, SaaS private, publice, hibride)?	0	-		-	

4.1.2 Clusterul #2: Consolidarea capacităților și acțiuni de sensibilizare

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
4 – Stabilirea unei capacități de reacție la incidente	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Dispuneți de capacități informale de răspuns la incidente gestionate în cadrul sectoarelor public și privat sau între acestea?	1	Aveți cel puțin un CSIRT național oficial?	1	Dispuneți de capacități de răspuns la incidente pentru sectoarele menționate în anexa II la Directiva NIS?	1	Ați definit și promovat practici standardizate pentru procedurile de răspuns la incidente și sistemele de clasificare a incidentelor?	1	Dispuneți de mecanisme de detectare timpurie, de identificare, de prevenire, de răspuns și de atenuare a vulnerabilităților de tip zero-day?	1
	2	-		CSIRT-ul/CSIRT-urile din țara dumneavoastră are/au un domeniu de intervenție clar definit (de exemplu, în funcție de sectorul vizat, de tipurile de incidente, de impacturi)?	1	Există un mecanism de cooperare CSIRT în țara dumneavoastră pentru a răspunde la incidente?	1	Vă evaluați capacitatea de răspuns la incidente pentru a vă asigura că dispuneți de resursele și competențele adecvate pentru a îndeplini sarcinile prevăzute la punctul (2) din anexa I la Directiva NIS?	1	-	
	3	-		CSIRT-ul/CSIRT-urile dumneavoastră național(e) au relații clar definite cu alte părți interesate de la nivel național în ceea ce privește peisajul național în materie de securitate cibernetică și practicile de răspuns în caz de incidente (de exemplu, AAL, autorități militare, ISP, NCSC)?	0	CSIRT-ul/CSIRT-urile dumneavoastră național(e) dispun(e) de o capacitate de răspuns la incidente în conformitate cu anexa I la Directiva NIS? (și anume, disponibilitate, securitate fizică, continuitatea activității, cooperare internațională, monitorizarea incidentelor, capacitate de alertă și avertizare timpurie, răspuns la incidente, analiza riscurilor și conștientizarea situației, cooperare cu sectorul privat, practici standard etc.)	1	-		-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
4 – Stabilirea unei capacități de reacție la incidente	4	-				Există un mecanism de cooperare cu alte țări învecinate în ceea ce privește incidentele?	1	-		-	
	5	-		-		Ați definit în mod oficial politici și proceduri clare de gestionare a incidentelor?	1	-		-	
	6	-		-		CSIRT-ul/CSIRT-urile dumneavoastră național(e) participă la exerciții de securitate cibernetică atât la nivel național, cât și la nivel internațional?	1	-		-	
	7	-		-		CSIRT-ul/CSIRT-urile dumneavoastră național(e) este (sunt) afiliată (afiliate) la FIRST (Forumul echipelor de securitate și de intervenție în caz de incidente)?	0	-		-	
5 – Sensibilizarea utilizatorilor	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Există o recunoaștere minimă din partea guvernului, a sectorului privat sau a utilizatorilor generali că este necesară sensibilizarea cu privire la aspectele legate de securitatea cibernetică și de protecția vieții private?	1	Ați identificat un public-țintă specific pentru sensibilizarea utilizatorilor? De exemplu, utilizatori generali, tineri, utilizatori comerciali (categorie care pot fi defalcată în continuare: IMM-uri, OSE, DSP etc.)	1	Ați elaborat planuri/strategii de comunicare pentru campanii?	1	Elaborați indicatori pentru evaluarea campaniei dumneavoastră în etapa de planificare?	1	Dispuneți de mecanisme care să garanteze că campaniile de sensibilizare sunt în permanență relevante în ceea ce privește progresul tehnologic, schimbările în peisajul amenințărilor, reglementările juridice și directivele în materie de securitate națională?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
5 – Sensibilizarea utilizatorilor	2	Agențiile publice desfășoară campanii ad-hoc de sensibilizare cu privire la securitatea cibernetică în cadrul organizației lor? (de exemplu, în urma unui incident de securitate cibernetică).	0	Elaborați un plan de proiect pentru a spori gradul de conștientizare cu privire la aspectele legate de securitatea informațiilor și de protecția vieții private?	1	Dispuneți de un proces de creare de conținut la nivel guvernamental?	1	Vă evaluați campaniile după execuție?	1	Efectuați evaluări sau studii periodice pentru a măsura schimbările de atitudine sau de comportament în ceea ce privește aspectele legate de securitatea cibernetică și de protecția vieții private în sectoarele public și privat?	1
	3	Agențiile publice desfășoară campanii ad-hoc de sensibilizare cu privire la securitatea cibernetică pentru publicul larg? (de exemplu, în urma unui incident de securitate cibernetică).	0	Dispuneți de resurse disponibile și ușor de identificat (de exemplu, un portal online unic, kituri de sensibilizare) pentru orice utilizator care încearcă să afle informații privind aspecte legate de securitatea cibernetică și de protecția vieții private?	1	Dispuneți de mecanisme de identificare a domeniilor-țintă pentru sensibilizarea publicului (și anume, Raportul ENISA privind situația amenințărilor, situațiile naționale, situațiile internaționale, feedbackul din partea centrelor naționale de combatere a criminalității informatice etc.)?	1	Dispuneți de mecanisme de identificare a celor mai relevante mijloace de comunicare sau canale de comunicare, în funcție de publicul-țintă, pentru a maximiza gradul de informare și de implicare? (de exemplu, diferite tipuri de mass-media digitală, broșuri, e-mailuri, materiale didactice, afișe în zone aglomerate, TV, radio etc.)	1	Consultați experți în materie de comportament pentru a vă adapta campania la publicul-țintă?	1
	4	-		-		Reuniți părțile interesate cu experți și echipe de comunicare pentru a crea conținut?	1			-	
	5	-		-		Implicați și angajați sectorul privat în eforturile dumneavoastră de sensibilizare pentru a promova și a difuza mesajele către un public mai larg?	1	-		-	
	6	-		-		Pregătiți inițiative specifice de sensibilizare pentru cadrele de conducere din sectoarele public, privat, academic sau al societății civile?	1	-		-	
	7	-		-		Participați la campaniile ENISA privind Luna europeană a securității cibernetice (ECSM)?	0	-		-	
6 – Organizarea de exerciții de securitate cibernetică	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
6 – Organizarea de exerciții de securitate cibernetică	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Efectuați exerciții de criză în alte sectoare (altele decât securitatea cibernetică) la nivel național sau paneuropean?	1	Dispuneți de un program de exerciții de securitate cibernetică la nivel național?	1	Implicați toate autoritățile competente din administrația publică? (chiar dacă scenariul este specific sectorului)	1	Redactați rapoarte de acțiune/rapoarte de evaluare?	1	Aveți o capacitate de analiză a învățămintelor desprinse în domeniul cibernetic (procese de raportare, analiză, atenuare)?	1
	2	Dispuneți de resurse alocate pentru conceperea și planificarea exercițiului de gestionare a crizelor?	1	Efectuați sau prioritizați exercițiile de gestionare a crizelor cibernetice cu privire la funcțiile societale vitale și la infrastructura critică?	1	Implicați sectorul privat în planificarea și realizarea exercițiilor?	1	Testați planuri și proceduri la nivel național?	1	Aveți un proces consacrat privind învățămintele desprinse?	1
	3	-		Ați identificat un organism de coordonare care să supravegheze conceperea și planificarea exercițiilor de securitate cibernetică (agenție publică, consultanță etc.)?	0	Organizați exerciții sectoriale specifice la nivel național și/sau internațional?	1	Participați la exerciții de securitate cibernetică la nivel paneuropean?	1	Adaptați scenariile de exerciții în funcție de cele mai recente evoluții (progrese tehnologice, conflicte globale, situația amenințărilor etc.)?	1
	4	-		-		Organizați exerciții în toate sectoarele critice menționate în anexa II la Directiva NIS?	1	-		Vă aliniați procedurile de gestionare a crizelor cu cele din alte state membre pentru a asigura gestionarea eficace a crizelor la nivel paneuropean?	1
	5	-		-		Organizați exerciții de securitate cibernetică intersectoriale și/sau transsectoriale?	1	-		Dispuneți de un mecanism pentru a adapta rapid strategia, planurile și procedurile din învățămintele desprinse în timpul exercițiilor?	0
	6	-		-		Organizați exerciții de securitate cibernetică specifice la diferite niveluri? (nivel tehnic și operațional, nivel procedural, nivel decizional, nivel politic etc.)	0	-		-	
7 – Consolidarea programelor de formare și educaționale	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să-l includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	1	Aveți în vedere dezvoltarea de programe educaționale și de formare în domeniul securității cibernetice?	1	Organizați cursuri de formare dedicate securității cibernetice?	1	Țara dumneavoastră înglobează cultura securității cibernetice încă din primele etape ale parcursului educațional al studenților? De exemplu, sunteți în favoarea securității cibernetice în școlile generale și licee?	1	Solicitați ca personalul din sectorul public și privat să fie acreditat sau certificat?	1	Dispuneți de mecanisme prin care să vă asigurați că programele educaționale și de formare sunt în permanență relevante în ceea ce privește evoluțiile tehnologice actuale și emergente, schimbările în peisajul amenințărilor, reglementările juridice și directivele naționale în materie de securitate?	1
	2	-		Universitățile din țara dumneavoastră oferă programe de doctorat în domeniul securității cibernetice ca disciplină independentă și nu ca subiect al științelor informatice?	1	Aveți laboratoare naționale de cercetare și instituții de învățământ specializate în securitatea cibernetică?	1	Țara dumneavoastră a elaborat programe de formare sau de mentorat în domeniul securității cibernetice pentru a sprijini întreprinderile nou-înființate și IMM-urile naționale?	1	Înființați centre academice de excelență în materie de securitate cibernetică pentru a acționa ca centre de cercetare și educație?	1
	3	-		Intenționați să formați educatori, indiferent de domeniul lor de activitate, cu privire la aspecte legate de securitatea informațiilor și de protecția vieții private? (de exemplu, siguranța online, protecția datelor cu caracter personal, hărțuirea pe internet).	1	Încurajați/finanțați cursuri specifice de securitate cibernetică și planuri de formare pentru angajații agențiilor de ocupare a forței de muncă din statele membre?	1	Promovați în mod activ adăugarea de cursuri de securitatea informațiilor în învățământul superior nu numai pentru studenții din domeniul informaticii, ci și pentru orice altă specialitate profesională? (de exemplu, cursuri adaptate nevoilor profesiei respective).	1	Participă instituțiile academice la conducerea dezbaterilor în domeniul educației și cercetării în materie de securitate cibernetică la nivel internațional?	0
	4	-		-		Dispuneți de cursuri de securitate cibernetică și/sau de o programă de învățământ specializată pentru nivelul 5-8 al CEC (Cadrul european al calificărilor)?	1	Evaluați în mod regulat lacunele în materie de competențe (deficitul de lucrători în domeniul securității cibernetice) în domeniul securității informațiilor?	1	-	
	5	-		-		Încurajați și/sau sprijiniți inițiativele de includere a cursurilor privind siguranța internetului în învățământul primar și secundar?	1	Încurajați crearea de rețele și schimbul de informații între instituțiile academice, atât la nivel național, cât și la nivel internațional?	1		

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
7 - Consolidarea programelor de formare și educaționale	6	-		-		Finanțați sau oferiți gratuit cetățenilor cursuri de formare de bază în materie de securitate cibernetică?	0	Implicați sectorul privat sub orice formă în inițiativele de educare în privința securității cibernetice? (de exemplu, conceperea și predarea cursurilor, stagii, stagii în întreprindere etc.)	1	-	
	7	-		-		Organizați evenimente anuale privind securitatea informațiilor (de exemplu, concursuri de hacking sau maratoane de hacking)?	0	Aplicați mecanisme de finanțare pentru a încuraja adoptarea diplomelor de securitate cibernetică? (de exemplu, burse, stagii de ucenicie/stagii garantate, locuri de muncă garantate în anumite sectoare sau roluri în sectorul public)	0	-	
8 – Promovarea cercetării și dezvoltării (C&D)	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să-l includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați efectuat studii sau analize pentru a identifica prioritățile C&D în materie de securitate cibernetică?	1	Dispuneți de un proces de definire a priorităților C&D (de exemplu, teme emergente pentru descurajarea, protejarea, detectarea și adaptarea la noi tipuri de atacuri informatice)?	1	Există un plan de corelare a inițiativelor C&D cu economia reală?	1	Sunt conforme inițiativele C&D în materie de securitate cibernetică cu obiectivele strategice relevante, de exemplu DSM, H2020, Europa digitală, Strategia UE în materie de securitate cibernetică?	1	Urmăriți la nivel național cooperarea cu orice inițiative internaționale C&D legate de securitatea cibernetică?	1
	2	-		Este sectorul privat implicat în stabilirea priorităților C&D?	1	Există proiecte naționale legate de securitatea cibernetică?	1	Există un sistem de evaluare pentru inițiativele C&D?	1	Prioritățile C&D sunt aliniate cu reglementările actuale sau viitoare (la nivel național)?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
8 – Promovarea cercetării și dezvoltării (C&D)	3	-		Este implicat mediul academic în stabilirea priorităților C&D?	1	Dispuneți de ecosisteme locale/regionale ale întreprinderilor nou-înființate și de alte canale de creare de rețele (de exemplu parcuri tehnologice, clustere de inovare, evenimente/platforme de creare de rețele) pentru a stimula inovarea (inclusiv pentru întreprinderile nou-înființate în domeniul securității cibernetice)?	1	Există acorduri de cooperare cu universități și alte centre de cercetare?	1	Participați la conducerea dezbaterilor cu privire la una sau mai multe teme de C&D avansate la nivel internațional?	0
	4	-		Există inițiative naționale de C&D legate de securitatea cibernetică?	0	Există investiții în programe C&D în domeniul securității cibernetice în mediul academic și în sectorul privat?	1	Există un organism instituțional recunoscut care supraveghează activitățile C&D în materie de securitate cibernetică?	0	-	
	5	-		-		Dispuneți de catedre de cercetare industrială în universități pentru a face legătura între subiectele de cercetare și nevoile pieței?	1	-		-	
	6	-		-		Dispuneți de programe specifice de finanțare C&D pentru securitatea cibernetică?	0	-		-	
9 – Oferirea de stimulente pentru ca sectorul privat să investească în măsuri de securitate	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Există o politică industrială sau o voință politică de a încuraja dezvoltarea sectorului securității cibernetice?	1	Este sectorul privat implicat în conceperea stimulentelor?	1	Există stimulente economice/de reglementare sau alte tipuri de stimulente pentru a promova investițiile în securitatea cibernetică?	1	Există actori privați care reacționează la stimulente prin investiții în măsuri de securitate? (de exemplu, investitori specializați în securitatea cibernetică și investitori nespecializați)	1	Vă concentrați stimulentele pe teme legate de securitatea cibernetică, în funcție de cele mai recente evoluții ale amenințărilor?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
9 – Oferirea de stimulente pentru ca sectorul privat să investească în măsuri de securitate	2	-		Ați identificat teme specifice în materie de securitate cibernetică care urmează să fie dezvoltate? (de exemplu, criptografia, protejarea vieții private, noua formă de autentificare, IA pentru securitatea cibernetică etc.)	0	Oferiți sprijin (de exemplu, stimulente fiscale) pentru întreprinderile nou-înființate și IMM-urile din domeniul securității cibernetice?	1	Oferiți stimulente pentru ca sectorul privat să se concentreze asupra securității tehnologiilor de vârf? (de exemplu, 5G, inteligența artificială, IoT, sistemul de calcul cuantic etc.)	1	-	
	3	-		-		Oferiți stimulente fiscale sau alte stimulente financiare investitorilor din sectorul privat în întreprinderile nou-înființate în domeniul securității cibernetice?	1	-		-	
	4	-		-		Facilitați accesul întreprinderilor nou-înființate și al IMM-urilor în domeniul securității cibernetice la procesul de achiziții publice?	0	-		-	
	5	-		-		Există un buget disponibil pentru a oferi stimulente sectorului privat?	0	-		-	
10 – Îmbunătățirea securității cibernetice a lanțului de aprovizionare	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați realizat un studiu privind bunele practici în materie de securitate pentru gestionarea lanțului de aprovizionare utilizate în cadrul achizițiilor publice în diferite segmente ale industriei și/sau în sectorul public?	1	Efectuați evaluări ale securității cibernetice de-a lungul întregului lanț de aprovizionare cu servicii și produse TIC în sectoare critice [astfel cum sunt identificate în anexa II la Directiva privind securitatea rețelelor și a informațiilor (2016/1148)]?	1	Utilizați un sistem de certificare de securitate pentru produsele și serviciile bazate pe TIC? (de exemplu ARR SOG-IS în Europa (Grupul înalților funcționari pentru securitatea sistemelor informatice, acordul de recunoaștere reciprocă), Acordul privind recunoașterea criteriilor comune (CCRA), inițiativele naționale, inițiativele sectoriale etc.)	1	Dispuneți de un proces de actualizare a evaluărilor de securitate cibernetică ale lanțului de aprovizionare cu servicii și produse TIC în sectoare critice [astfel cum sunt identificate în anexa II la Directiva privind securitatea rețelelor și a informațiilor (2016/1148)]?	1	Dispuneți de sonde de detectare a elementelor-cheie din lanțul de aprovizionare pentru a detecta semnele timpurii de compromitere? (de exemplu, controale de securitate la nivelul ISP, sonde de securitate în componentele majore ale infrastructurii etc.)	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
10 – Îmbunătățirea securității cibernetice a lanțului de aprovizionare	2	-		Aplicați standarde în politicile de achiziții publice ale administrațiilor publice pentru a asigura că furnizorii de produse sau servicii TIC îndeplinesc cerințele de bază în materie de securitate a informațiilor? (de exemplu, ISO/IEC 27001 și 27002, ISO/IEC 27036 etc.)	1	Promovați activ cele mai bune practici în dezvoltarea de produse și servicii TIC în materie de securitate și de protejare a vieții private din faza de concepere? (de exemplu, ciclul de viață al dezvoltării de software securizat, ciclul de viață al internetului obiectelor)	1	Dispuneți de un proces de identificare a verigilor slabe în materie de securitate cibernetică din lanțul de aprovizionare al sectoarelor esențiale [astfel cum sunt identificate în anexa II la Directiva privind securitatea rețelelor și a informațiilor (2016/1148)]?	1	-	
	3	-		-		Dezvoltați și furnizați cataloage centralizate cu informații extinse privind standardele existente în materie de securitate a informațiilor și de protecție a vieții private, care pot fi extinse pentru IMM-uri și pot fi aplicate de către acestea?	1	Dispuneți de mecanisme pentru a vă asigura că produsele și serviciile TIC care sunt esențiale pentru OSE sunt reziliente din punct de vedere cibernetic (și anume, capacitatea de a menține disponibilitatea și siguranța împotriva unui incident cibernetic)? (de exemplu, prin testare, evaluări periodice, detectarea elementelor compromise etc.)	1	-	
	4	-				Participați activ la elaborarea unui cadru UE de certificare pentru produsele, serviciile și procesele digitale TIC, astfel cum este stabilit în Regulamentul UE privind securitatea cibernetică [Regulamentul (UE) 2019/881]? (de exemplu, participarea la Grupul european pentru certificarea securității cibernetice (ECCG), promovarea standardelor și procedurilor tehnice pentru securitatea produselor/serviciilor TIC)	0	Promovați dezvoltarea unor sisteme de certificare destinate IMM-urilor pentru a stimula adoptarea standardelor în materie de securitate a informațiilor și de protecție a vieții private?	0	-	
	5	-		-		Oferiți vreun tip de stimulente IMM-urilor pentru ca acestea să adopte standarde de securitate și de protecție a vieții private?	0	Aveți în vigoare dispoziții pentru a încuraja întreprinderile mari să sporească securitatea cibernetică a întreprinderilor mici în lanțurile lor de aprovizionare? (de exemplu, platformă de securitate cibernetică, campanii de formare și de sensibilizare etc.)	0	-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	6	-		-		Încurajați furnizorii de software să sprijine IMM-urile prin asigurarea unor configurații implicite sigure în produsele destinate organizațiilor mici?	0	-		-	

4.1.3 Clusterul #3: Aspecte juridice și de reglementare

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
11 – Protejarea infrastructurilor critice de informații, a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP)	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Există o înțelegere generală conform căreia operatorii infrastructurilor critice de informații contribuie la securitatea națională?	1	Dispuneți de o metodologie de identificare a serviciilor esențiale?	1	Ați pus în aplicare Directiva privind securitatea rețelelor și a informațiilor (2016/1148)?	1	Dispuneți de o procedură de actualizare a registrului riscurilor?	1	Creați și actualizați rapoarte privind situația amenințărilor?	1
	2	-		Dispuneți de o metodologie pentru identificarea infrastructurilor critice de informații?	1	Ați pus în aplicare Directiva infrastructurilor critice europene (2008/114) privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora?	1	Dispuneți de alte mecanisme pentru a evalua dacă măsurile tehnice și organizatorice puse în aplicare de OSE sunt adecvate pentru gestionarea riscurilor la adresa securității rețelelor și a sistemelor informatice? (de exemplu, audituri periodice de securitate cibernetică, cadrul național pentru punerea în aplicare a măsurilor standard, instrumentele tehnice furnizate de guvern, cum ar fi sondele de detectare sau analiza configurației specifice sistemului etc.)	1	În funcție de cele mai recente evoluții din situația amenințărilor, sunteți în măsură să includeți un nou sector în planul dumneavoastră de acțiune privind protecția infrastructurilor critice de informație?	1
	3	-		Dispuneți de o metodologie de identificare a OSE?	1	Dispuneți de un registru național pentru OSE identificate pentru fiecare sector critic?	1	Revizuiți și actualizați în consecință lista OSE identificate cel puțin o dată la doi ani?	1	În funcție de ultimele evoluții din situația amenințărilor, sunteți în măsură să adaptați noile cerințe din planul dumneavoastră de acțiune privind protecția infrastructurilor critice de informație?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
11 – Protejarea infrastructurilor critice de informații, a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP)	4	-		Dispuneți de o metodologie de identificare a furnizorilor de servicii digitale?	1	Dispuneți de un registru național pentru furnizorii de servicii digitale identificați?	1	Dispuneți de alte mecanisme pentru a evalua dacă măsurile tehnice și organizatorice puse în aplicare de furnizorii de servicii digitale sunt adecvate pentru gestionarea riscurilor la adresa securității rețelelor și a sistemelor informatice? (de exemplu, audituri periodice de securitate cibernetică, cadrul național pentru punerea în aplicare a măsurilor standard, instrumentele tehnice furnizate de guvern, cum ar fi sondele de detectare sau analiza configurației specifice sistemului etc.)	1	-	
	5	-		Aveți una sau mai multe autorități naționale care asigură supravegherea protecției infrastructurilor critice de informații și a securității rețelelor și a sistemelor informatice? [de exemplu, în conformitate cu Directiva privind securitatea rețelelor și a informațiilor (2016/1148)]	1	Dispuneți de un registru național al riscurilor pentru riscurile identificate sau cunoscute?	1	Revizuiți și actualizați în consecință lista furnizorilor de servicii digitale identificați cel puțin o dată la doi ani?	1	-	
	6	-		Elaborați planuri de protecție specifice fiecărui sector? [de exemplu, inclusiv măsuri de referință în materie de securitate cibernetică (obligatorii sau orientări)]	0	Dispuneți de o metodologie de cartografiere a dependențelor infrastructurilor critice de informații?	1	Utilizați un sistem de certificare de securitate (național sau internațional) pentru a ajuta OSE și furnizorii de servicii digitale să identifice produse TIC sigure? (de exemplu, SOG-IS MRA în Europa, inițiative naționale etc.)	1	-	
	7	-		-		Utilizați practici de gestionare a riscurilor pentru a identifica, a cuantifica și a gestiona riscurile legate de infrastructurile critice de informații la nivel național?	1	Utilizați un sistem de certificare de securitate sau o procedură de calificare pentru a evalua furnizorii de servicii care lucrează cu OSE? (de exemplu, furnizori de servicii în domeniul detectării incidentelor, al răspunsului în caz de incidente, al auditului securității cibernetice, al serviciilor cloud, al cardurilor inteligente etc.)	1	-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
11 – Protejarea infrastructurilor critice de informații, a operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (DSP)	8	-		-		Participați la un proces de consultare pentru a identifica dependențele transfrontaliere?	1	Dispuneți de mecanisme pentru a măsura nivelul de conformitate al OSE și al furnizorilor de servicii digitale în ceea ce privește măsurile de referință în materie de securitate cibernetică?	0	-	
	9					Dispuneți de un punct unic de contact responsabil de coordonarea aspectelor legate de securitatea rețelelor și a sistemelor informatice la nivel național și de cooperarea transfrontalieră la nivelul Uniunii?	1	Aveți în vigoare dispoziții pentru a asigura continuitatea serviciilor furnizate de infrastructurile critice de informații? (de exemplu, anticiparea crizelor, proceduri de reconstruire a sistemelor informatice critice, continuitatea activității fără TI, proceduri de rezervă protejate prin „air gap”, neconectate la Internet etc.)	0		
	10					Definiți măsuri de referință în materie de securitate cibernetică (obligatorii sau orientări) pentru furnizorii de servicii digitale și pentru toate sectoarele identificate în anexa II la Directiva privind securitatea rețelelor și a informațiilor (2016/1148)?	1				
	11	-		-		Furnizați instrumente sau metodologii pentru detectarea incidentelor cibernetice?	1	-		-	
12 – Combaterea criminalității cibernetice	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
12 – Combaterea criminalității cibernetice	1	Ați efectuat un studiu pentru a identifica cerințele în materie de aplicare a legii (temei juridic, resurse, competențe etc.) pentru a combate în mod eficace criminalitatea informatică?	1	Cadrul juridic național din țara dumneavoastră respectă pe deplin cadrul juridic relevant al UE, inclusiv Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice? (de exemplu, accesarea ilegală a sistemelor informatice, afectarea integrității unui sistem, afectarea integrității datelor, interceptarea ilegală, instrumentele care servesc la săvârșirea infracțiunilor etc.)	1	Dispuneți de unități dedicate combaterii criminalității informatice în cadrul parchetelor?	1	Colectați statistici în conformitate cu dispozițiile articolului 14 alineatul (1) din Directiva 2013/40/UE (Directiva privind atacurile împotriva sistemelor informatice)?	1	Dispuneți de cursuri de formare interinstituțională sau ateliere de formare pentru autoritățile de aplicare a legii, judecători, procurori și echipe CSIRT naționale/guvernamentale la nivel național și/sau multilateral?	1
	2	Ați efectuat un studiu pentru a identifica cerințele aplicabile procurorilor și ale judecătorilor (temei juridic, resurse, competențe etc.) pentru a combate în mod eficace criminalitatea informatică?	1	Dispuneți de o dispoziție legală privind furtul de identitate și furtul de date cu caracter personal în mediul online?	1	Dispuneți de un buget dedicat unităților de combatere a criminalității informatice?	1	Colectați statistici separate privind criminalitatea informatică?(de exemplu statistici operaționale, statistici privind tendințele în domeniul criminalității informatice, statistici privind veniturile obținute din criminalitatea informatică și daunele cauzate etc.)	1	Participați la acțiuni coordonate la nivel internațional pentru contracararea activităților infracționale? (de exemplu, infiltrarea forumurilor de intruziune informatică infracțională, a grupurilor de criminalitate informatică organizată, închiderea piețelor criptate și a botneturilor etc.)	1
	3	Țara dumneavoastră a semnat Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică?	1	Dispuneți de dispoziții legale privind încălcările drepturilor de proprietate intelectuală și a drepturilor de autor în mediul online?	1	Ați înființat un organism/o entitate centrală pentru coordonarea activităților în domeniul combaterii criminalității informatice?	1	Evaluați caracterul adecvat al formării oferite autorităților de aplicare a legii, sistemului judiciar și personalului echipei (echipelor) CSIRT naționale pentru combaterea criminalității cibernetice?	1	Există o separare clară a sarcinilor între echipele CSIRT, autoritățile de aplicare a legii și sistemul judiciar (procurori și judecători) atunci când cooperează pentru abordarea infracțiunilor informatice?	1
	4			Dispuneți de dispoziții juridice care abordează hărțuirea online sau hărțuirea pe internet?	1	Ați instituit mecanisme de cooperare între instituțiile naționale relevante implicate în combaterea criminalității informatice, inclusiv echipe CSIRT naționale de aplicare a legii?	1	Efectuați evaluări periodice pentru a vă asigura că dispuneți de suficiente resurse (umane, bugetare și instrumente) dedicate unităților de combatere a criminalității informatice din cadrul autorităților de aplicare a legii?	1	Cadrul dumneavoastră de reglementare facilitează cooperarea dintre CSIRT/autoritățile de aplicare a legii și sistemul judiciar (procurori și judecători)?	1
	5			Aveți dispoziții juridice care să abordeze frauda informatică? (de exemplu, respectarea prevederilor Convenției de la Budapesta a Consiliului Europei privind criminalitatea informatică)	1	Cooperați și partajați informații cu alte state membre în domeniul combaterii criminalității informatice?	1	Efectuați evaluări periodice pentru a vă asigura că dispuneți de suficiente resurse (umane, bugetare și instrumente) dedicate unităților de combatere a criminalității informatice din cadrul autorităților de urmărire penală?	1	Participați la elaborarea și menținerea unor instrumente și metodologii standardizate, formulare și proceduri care să fie partajate cu părțile interesate din UE (autorități de aplicare a legii, echipe CSIRT, ENISA, EC3 al Europol etc.)?	1

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
12 – Combaterea criminalității cibernetice	6	-		Dispuneți de dispoziții juridice privind protecția online a copiilor? (de exemplu, respectarea dispozițiilor Directivei 2011/93/UE și ale Convenției de la Budapesta a Consiliului Europei privind criminalitatea informatică etc.)	1	Cooperați și faceți schimb de informații cu agențiile UE (de exemplu EC3 al Europol, Eurojust, ENISA) în domeniul combaterii criminalității informatice?	1	Dispuneți de unități, instanțe specializate sau judecători specializați care să se ocupe de cazurile de criminalitate informatică?	1	Dispuneți de mecanisme avansate pentru a descuraja persoanele să fie atrase sau implicate în criminalitatea informatică?	0
	7	-		Ați identificat un punct de contact național operațional pentru schimbul de informații și pentru a răspunde solicitărilor urgente de informații din partea altor state membre cu privire la infracțiunile prevăzute în Directiva 2013/40/UE (Directiva privind atacurile împotriva sistemelor informatice)?	1	Dispuneți de instrumentele adecvate pentru combaterea criminalității cibernetice? (de exemplu, taxonomia și clasificarea criminalității informatice, instrumente de colectare a probelor electronice, instrumente de criminalistică informatică, platforme de partajare de încredere etc.)	1	Dispuneți de dispoziții dedicate furnizării de sprijin și asistență victimelor infracțiunilor informatice (utilizatori generali, IMM-uri, întreprinderi mari)?	1	Utilizează țara dumneavoastră Planul UE și/sau Protocolul UE privind răspunsul în caz de urgență al autorităților de aplicare a legii (Law Enforcement Emergency Response Protocol - EU LE ERP) pentru a răspunde în mod eficace la incidentele cibernetice de mare amploare?	0
	8			Agenția dumneavoastră de aplicare a legii include o unitate dedicată criminalității informatice?	1	Dispuneți de proceduri standard de operare pentru a gestiona probele electronice?	1	Ați instituit un cadru interinstituțional și mecanisme de cooperare între toate părțile interesate relevante (de exemplu, autoritățile de aplicare a legii, CSIRT naționale, comunitățile judiciare), inclusiv sectorul privat (de exemplu, operatorii de servicii esențiale, furnizorii de servicii), după caz, pentru a răspunde atacurilor cibernetice?	1	-	
	9			Ați desemnat, în conformitate cu articolul 35 din Convenția de la Budapesta, un punct de contact care este disponibil 24 de ore din 24, 7 zile din 7?	1	Participă țara dumneavoastră la oportunitățile de formare oferite și/sau sprijinite de agențiile UE (de exemplu, Europol, Eurojust, OLAF, CEPOL, ENISA)?	0	Cadrul dumneavoastră de reglementare facilitează cooperarea dintre echipele CSIRT și autoritățile de aplicare a legii?	1	-	
	10	-		Ați desemnat un punct național de contact operațional care este disponibil 24 de ore din 24, 7 zile din 7 pentru Protocolul UE privind răspunsul în caz de urgență al autorităților de aplicare a legii (EU LE ERP) pentru a răspunde la atacuri cibernetice majore?	1	Intenționează țara dumneavoastră să adopte cel de al 2-lea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică?	0	Dispuneți de mecanisme (de exemplu, instrumente, proceduri) pentru a facilita schimbul de informații și cooperarea dintre CSIRT/autoritățile de aplicare a legii și, eventual, sistemul judiciar (procurori și judecători) în domeniul combaterii criminalității informatice?	1	-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	11			Oferiți în mod regulat cursuri de formare specializate părților interesate implicate în combaterea criminalității informatice (autorități de aplicare a legii, sistemul judiciar, CSIRT)? (de exemplu, sesiuni de formare privind sesizarea/urmărirea penală a infracțiunilor înlesnite informatic, cursuri de formare privind colectarea de probe electronice și asigurarea integrității de-a lungul întregului lanț digital de custodie și criminalistică informatică, printre altele)	1						
	12			Țara dumneavoastră a ratificat/aderat la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică?	1			-	-	-	
	13	-		Țara dumneavoastră a semnat și a ratificat Protocolul adițional (incriminarea actelor de natură rasistă și xenofobă comise prin intermediul sistemelor informatice) la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică?	0	-	-	-		-	
13 – Instituirea unor mecanisme de raportare a incidentelor	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
13 – Instituirea unor mecanisme de raportare a incidentelor	1	Dispuneți de mecanisme informale de schimb de informații privind incidentele de securitate cibernetică între organizațiile private și autoritățile naționale?	1	Dispuneți de un sistem de raportare a incidentelor pentru toate sectoarele în temeiul anexei II la Directiva NIS?	1	Dispuneți de un sistem obligatoriu de raportare a incidentelor care funcționează în practică?	1	Dispuneți de o procedură armonizată pentru sistemele sectoriale de raportare a incidentelor?	1	Creați un raport anual privind incidentele?	1
	2	-		Ați pus în aplicare cerințele de notificare pentru furnizorii de servicii de telecomunicații în conformitate cu articolul 40 din Directiva (UE) 2018/1972? Directiva impune statelor membre să se asigure că furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului notifică fără întârziere autorității competente un incident de securitate care a avut un impact semnificativ asupra funcționării rețelelor sau serviciilor.	1	Există un mecanism de coordonare/cooperare pentru obligațiile de raportare a incidentelor în ceea ce privește RGPD, Directiva NIS, articolul 40 (fostul articol 13a) și eIDAS?	1	Dispuneți de un sistem de raportare a incidentelor pentru alte sectoare decât cele prevăzute de Directiva NIS?	1	Există rapoarte privind situația securității cibernetice sau alte tipuri de analize pregătite de entitatea care primește rapoartele privind incidentele?	1
	3	-		Ați pus în aplicare cerințele de notificare pentru prestatorii de servicii de asigurare a încrederii în conformitate cu articolul 19 din Regulamentul eIDAS [Regulamentul (UE) nr. 910/2014]? Articolul 19 prevede, printre alte cerințe, ca prestatorii de servicii de asigurare a încrederii să notifice organismului de supraveghere incidentele/încălcările semnificative.	1	Dispuneți de instrumentele adecvate pentru a asigura confidențialitatea și integritatea informațiilor partajate prin intermediul diferitelor canale de raportare?	1	Evaluați eficacitatea procedurilor de raportare a incidentelor? (de exemplu, indicatori privind incidentele care au fost raportate prin canalele adecvate, calendarul raportului privind incidentele etc.)	1	-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
14 – Consolidarea protecției vieții private și a datelor	4	-		Ați pus în aplicare cerințele de notificare pentru furnizorii de servicii digitale în conformitate cu articolul 16 din Directiva NIS? Articolul 16 prevede obligația furnizorilor de servicii digitale de a notifica autorității competente sau CSIRT naționale, fără întârzieri nejustificate, orice incident care are un impact substanțial asupra furnizării unui serviciu, astfel cum se menționează în anexa III, pe care îl oferă în cadrul Uniunii.	1	Dispuneți de o platformă/un instrument care să faciliteze procesul de raportare?	0	Dispuneți de o taxonomie comună la nivel național pentru clasificarea incidentelor și a categoriilor de cauze principale?	0	-	
	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Ați efectuat studii sau analize pentru a identifica domeniile în care se pot aduce îmbunătățiri în vederea unei mai bune protecții a drepturilor la viața privată a cetățenilor?	1	Este implicată autoritatea națională de protecție a datelor în domenii legate de securitatea cibernetică (de exemplu, elaborarea de noi legi și reglementări în materie de securitate cibernetică, măsuri minime de securitate definite)?	1	Promovați cele mai bune practici privind măsurile de securitate și protecția datelor din faza de concepere pentru sectorul public și/sau privat?	1	Efectuați evaluări periodice pentru a vă asigura că dispuneți de suficiente resurse (umane, bugetare și instrumente) dedicate autorității pentru protecția datelor?	1	Dispuneți de mecanisme de monitorizare a celor mai recente evoluții tehnologice în vederea adaptării orientărilor relevante și a dispozițiilor/obligațiilor juridice relevante?	1
	2	Ați elaborat un temei juridic la nivel național pentru a pune în aplicare Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679]? (de exemplu, să mențineți sau să introduceți dispoziții mai specifice sau limitări ale normelor din regulament)	0	-		Lansați programe de sensibilizare și de formare pe această temă?	1	Încurajați organizațiile și întreprinderile să se certifice în conformitate cu ISO/IEC 27701:2019 privind sistemul de management al informațiilor privind confidențialitatea (PIMS)?	1	Participați/promovați în mod activ inițiative C&D privind tehnologiile de protecție a vieții private (privacy enhancing technologies - PET)?	0

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	3	-		-		Coordonați procedurile de raportare a incidentelor cu Regulamentul privind protecția datelor?	1	-		-	
	4	-		-		Promovați și sprijiniți elaborarea de standarde tehnice privind securitatea informațiilor și protecția vieții private? Aceste standarde sunt adaptate în mod specific la întreprinderile mici și mijlocii (IMM-uri)?	0	-		-	
	5	-		-		Furnizați orientări practice și adaptabile pentru a sprijini diferite tipuri de operatori de date în ceea ce privește îndeplinirea cerințelor și obligațiilor legale în materie de protecție a vieții private și a datelor?	0	-		-	

4.1.4 Clusterul #4: Cooperare

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
15 – Stabilirea unui parteneriat public-privat (PPP)	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						
	1	Este, în general, înțeles că PPP-urile contribuie la creșterea nivelului de securitate cibernetică în țară prin diferite mijloace? (de exemplu, împărtășirea intereselor în dezvoltarea sectorului securității cibernetice, cooperarea în vederea construirii unui cadru de reglementare relevant în materie de securitate cibernetică, promovarea C&D etc.)	1	Dispuneți de un plan național de acțiune pentru stabilirea PPP-urilor?	1	Ați instituit parteneriate public-privat la nivel național?	1	Ați instituit parteneriate public-privat intersectoriale?	1	În funcție de cele mai recente evoluții tehnologice și de reglementare, sunteți în măsură să adaptați sau să creați PPP?	1
	2	-		Stabiliți un temei juridic sau contractual (legi specifice, acorduri privind nedivulgarea datelor, proprietate intelectuală) pentru a acoperi parteneriatele public-privat?	1	Ați instituit parteneriate public-privat sectoriale?	1	În cadrul parteneriatelor public-privat stabilite, vă axați, de asemenea, pe cooperarea public-public și pe cooperarea privat-privat?	1		
	3	-		-		Oferiți finanțare pentru crearea de parteneriate public-privat?	1	Promovați PPP în rândul întreprinderilor mici și mijlocii (IMM-uri)?	1	-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
15 – Stabilirea unui parteneriat public-privat (PPP)	4	-		-		Instituțiile publice coordonează PPP-urile în ansamblu? (și anume, un punct unic de contact din sectorul public care conduce și coordonează PPP, organismele publice convin în prealabil cu privire la ceea ce doresc să realizeze, orientări clare din partea administrațiilor publice cu privire la nevoile și limitările lor pentru sectorul privat etc.)	1	Evaluați rezultatele PPP-urilor?	1	-	
	5	-		-		Sunteți membru al parteneriatului contractual public-privat (PPPc) al Organizației Europene pentru Securitate Cibernetică (ECSO)?	0	-		-	
	6	-		-		Aveți unul sau mai multe PPP-uri care desfășoară activități CSIRT?	0	-		-	
	7					Aveți unul sau mai multe PPP-uri care se ocupă de aspecte legate de protecția infrastructurilor critice de informații?	0				
	8	-		-		Aveți unul sau mai multe PPP-uri care vizează sensibilizarea cu privire la securitatea cibernetică și dezvoltarea competențelor?	0	-		-	
16 – Instituționalizarea cooperării între agenții publice	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	1	Dispuneți de canale de cooperare informală între agențiile publice?	1	Dispuneți de un sistem național de cooperare axat pe securitatea cibernetică? (de exemplu, consilii consultative, grupuri de coordonare, forumuri, consilii, centre cibernetice sau reuniuni ale grupurilor de experți)	1	Participă autoritățile publice la programul de cooperare?	1	Vă asigurați că există canale de cooperare dedicate securității cibernetice cel puțin între următoarele organisme publice: serviciile de informații, autoritățile naționale de aplicare a legii, autoritățile de urmărire penală, actorii guvernamentali, echipele CSIRT naționale și armata?	1	Agențiile publice primesc informații minime uniforme cu privire la cele mai recente evoluții ale situației amenințărilor și la conștientizarea situației în materie de securitate cibernetică?	1
	2	-		-		Ați instituit platforme de cooperare pentru schimbul de informații?	1	Evaluați succesele și limitele diferitelor scheme de cooperare în ceea ce privește promovarea unei cooperări eficace?	1	-	
16 – Instituționalizarea cooperării între agenții publice	3	-		-		Ați definit domeniul de aplicare a platformelor de cooperare (de exemplu, sarcini și responsabilități, numărul de domenii problematice)?	1	-		-	
	4	-		-		Organizați reuniuni anuale?	1	-		-	
	5	-		-		Dispuneți de mecanisme de cooperare între autoritățile competente din toate regiunile geografice? (de exemplu, rețea de corespondenți în materie de securitate cibernetică pentru fiecare regiune, responsabil cu securitatea cibernetică în camerele economice regionale etc.)	1	-		-	
17 – Implicarea în cooperarea internațională (nu numai cu statele membre ale UE)	a	Includeți acest obiectiv în SNSC dvs. actuală sau intenționați să îl includeți în următoarea ediție?	1	Există practici sau activități informale care participă la atingerea obiectivului în mod necoordonat?	1	Dispuneți de un plan de acțiune care este definit și documentat în mod oficial?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a testa performanța acestuia?	1	Dispuneți de mecanisme care să garanteze că planul de acțiune este adaptat în mod dinamic la evoluțiile din domeniul mediului?	1
	b			Ați definit rezultatele scontate, principiile directoare sau activitățile-cheie ale planului dvs. de acțiune?	1	Aveți un plan de acțiune cu o alocare clară a resurselor și o guvernanță clară?	1	Vă revizuiți planul de acțiune în ceea ce privește obiectivul pentru a vă asigura că acesta este corect prioritizat și optimizat?	1		
	c			Dacă este relevant, planul dvs. de acțiune este pus în aplicare și este deja eficace la o scară limitată?	0						

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
17 – Implicarea în cooperarea internațională (nu numai cu statele membre UE)	1	Aveți o strategie de implicare internațională?	1	Aveți acorduri de cooperare cu alte țări (bilaterale, multilaterale) sau parteneri din alte țări? (de exemplu, schimb de informații, consolidarea capacităților, asistență etc.)	1	Faceți schimb de informații la nivel strategic? (de exemplu, politica la nivel înalt, percepția riscurilor etc.)	1	Agențiile publice naționale de securitate cibernetică din țara dumneavoastră sunt implicate în sisteme de cooperare internațională?	1	Conduceți discuții pe una sau mai multe teme din cadrul acordurilor multilaterale?	1
	2	Aveți canale de cooperare informală cu alte țări?	1	Dispuneți de un punct unic de contact care poate exercita o funcție de legătură pentru a asigura cooperarea transfrontalieră cu autoritățile statelor membre (grup de cooperare, rețeaua CSIRT etc.)?	1	Faceți schimb de informații la nivel tactic? (de exemplu, buletin al factorilor de amenințare, centre de schimb și analiză de informații (ISAC), TTP etc.)	1	Evaluați periodic rezultatele inițiativelor de cooperare internațională?	1	Conduceți dezbateri cu privire la unul sau mai multe subiecte din tratatele sau convențiile internaționale?	1
	3	Și-a exprimat conducerea publică intenția de a se angaja în cooperarea internațională în domeniul securității cibernetice?	1	Aveți persoane dedicate implicate în cooperarea internațională?	1	Faceți schimb de informații la nivel operațional? (de exemplu, informații privind coordonarea operațională, incidente în curs, capacitatea operațională inițială (IOC) etc.)	1	-		Conduceți dezbateri sau negocieri pe una sau mai multe teme în cadrul grupurilor internaționale de experți? [de exemplu, Comisia globală pentru stabilitatea spațiului cibernetic, Grupul de cooperare privind NIS al ENISA, Grupul ONU de experți guvernamentali în securitatea informațiilor (UNGEG) etc.]	1
	4	-		-		Participați la exerciții internaționale de securitate cibernetică?	1	-		-	
	5	-		-		Participați la inițiative internaționale de consolidare a capacităților? (de exemplu, cursuri de formare, dezvoltarea competențelor, elaborarea de proceduri standard etc.)	0	-		-	
	6	-		-		Ați încheiat acorduri de asistență reciprocă cu alte țări? (de exemplu, activități ale autorităților de aplicare a legii, proceduri judiciare, reciprocitatea capacităților de răspuns în caz de incidente, partajarea activelor în materie de securitate cibernetică etc.)	0	-		-	

Obiectiv SNSC	#	Nivelul 1	R	Nivelul 2	R	Nivelul 3	R	Nivelul 4	R	Nivelul 5	R
	7	-		-		Ați semnat sau ratificat tratate sau convenții internaționale în domeniul securității cibernetice? (de exemplu Codul internațional de conduită pentru securitatea informațiilor, Convenția privind criminalitatea informatică)	0	-		-	

4.2 ORIENTĂRI PENTRU UTILIZAREA CADRULUI

Această secțiune urmărește să ofere statelor membre o serie de orientări și recomandări pentru punerea în aplicare a cadrului și pentru completarea chestionarului. Recomandările enumerate mai jos derivă în principal din feedback-ul colectat în urma interviurilor cu reprezentanții statelor membre:

- **Anticiparea activităților de coordonare pentru colectarea datelor și consolidarea datelor.** Majoritatea statelor membre recunosc că efectuarea unui astfel de exercițiu de autoevaluare ar trebui să dureze aproximativ 15 zile de muncă/om. Pentru a efectua autoevaluarea, va trebui solicitată o gamă largă de părți interesate diferite. Prin urmare, se recomandă alocarea de timp pentru faza de pregătire în vederea identificării tuturor părților interesate relevante din cadrul organismelor guvernamentale, al agențiilor publice și al sectorului privat.
- **Identificarea unui organism central responsabil cu finalizarea autoevaluării la nivel național.** Întrucât colectarea de materiale pentru toți indicatorii NCAF ar putea implica multe părți interesate, se recomandă să existe un organism central sau o agenție centrală însărcinat(ă) cu finalizarea autoevaluării prin asigurarea legăturii și coordonarea cu toate părțile interesate relevante.
- **Utilizarea exercițiului de evaluare ca modalitate de a împărtăși și a comunica pe teme legate de securitatea cibernetică.** Lecțiile învățate împărtășite de statele membre au arătat că dezbaterile (indiferent dacă se prezintă sub forma unor interviuri individuale sau a unor ateliere colective) reprezintă o bună ocazie de a promova dialogul pe teme legate de securitatea cibernetică și de a face schimb de opinii comune și domenii de îmbunătățire. Pe lângă faptul că pune în lumină principalele realizări, partajarea rezultatelor poate contribui, de asemenea, la promovarea temelor legate de securitatea cibernetică.
- **Utilizarea SNSC ca domeniu de aplicare pentru a selecta obiectivele care fac obiectul evaluării.** Cele 17 obiective care alcătuiesc NCAF au fost elaborate pe baza obiectivelor vizate în mod obișnuit de statele membre în cadrul SNSC. Obiectivele vizate ca parte a SNSC ar trebui să fie utilizate ca mijloc pentru a delimita domeniul de aplicare a evaluării. Cu toate acestea, SNSC nu ar trebui să limiteze evaluarea. Întrucât SNSC se concentrează în mod natural pe priorități, anumite domenii sunt omise intenționat din SNSC. Totuși, aceasta nu înseamnă că nu există o anumită capacitate. De exemplu, în cazul în care un obiectiv specific este omis din SNSC, dar țara are capabilități în materie de securitate cibernetică legate de obiectivul respectiv, se poate efectua evaluarea obiectivului respectiv.
- **Atunci când domeniul de aplicare a SNSC evoluează, asigurați-vă că interpretarea punctajului rămâne coerentă cu evoluția SNSC.** Ciclul de viață al SNSC este un proces multianual. SNSC ale unor state membre sunt puse în aplicare, de regulă, cu o foaie de parcurs de 3-5 ani, cu modificări ale domeniului de aplicare între două ediții succesive ale SNSC. În acest sens, trebuie să se acorde o atenție deosebită prezentării rezultatelor autoevaluării între două ediții ale SNSC: modificările domeniului de aplicare ar putea, într-adevăr, să aibă un impact asupra punctajului final pentru maturitate. Se recomandă compararea punctajelor pentru întregul domeniu de aplicare a obiectivelor strategice de la un an la altul (și anume, scorul general global).

Atenționare privind mecanismul de punctare – exemplu privind rata de acoperire
Mecanismul de punctare include două niveluri de punctaj:
(i) **o rată de acoperire generală globală** bazată pe lista completă a obiectivelor strategice prezente în cadrul de autoevaluare și
(ii) **o rată de acoperire specifică globală** bazată pe obiective strategice selectate de statul membru (care corespund, de regulă, obiectivelor prezente în SNSC a țării respective).

Din faza de concepție (a se vedea secțiunea 3.1 privind mecanismul de punctare), rata de acoperire specifică globală va fi egală sau mai mare decât rata de acoperire generală globală,

întrucât aceasta din urmă poate include obiective care nu sunt acoperite de statul membru, reducând astfel rata de acoperire generală globală. Atunci când un stat membru adaugă un nou obiectiv, rata de acoperire globală va crește (și anume, mai mulți indicatori de maturitate acoperiți), în timp ce maturitatea specifică globală poate scădea (în cazul în care obiectivul nou adăugat se află într-un stadiu incipient și, prin urmare, are un nivel scăzut de maturitate).

- **Atunci când completați chestionarul de autoevaluare, țineți seama de faptul că obiectivul principal este de a sprijini statele membre în consolidarea capacităților în materie de securitate cibernetică.** Prin urmare, atunci când se completează autoevaluarea, chiar dacă în anumite situații poate fi dificil să se răspundă la întrebare într-un mod clar, se recomandă alegerea răspunsului care este cel mai general acceptat. În cazul în care, de exemplu, răspunsul la o întrebare este DA la un anumit domeniu de aplicare, dar NU la un alt domeniu de aplicare, statele membre ar trebui să țină seama de faptul că un răspuns NU necesită o acțiune: fie un plan de reabilitare, fie un plan de acțiune privind un domeniu de îmbunătățire care trebuie luat în considerare în cadrul evoluțiilor viitoare.

5. ETAPELE URMĂTOARE

5.1 ÎMBUNĂTĂȚIRI VIITOARE

În cursul interviurilor cu reprezentanții statelor membre și în timpul etapei de cercetare documentară, următoarele recomandări de îmbunătățire a cadrului național actual de evaluare a capacităților au fost identificate, de asemenea, ca posibile evoluții viitoare:

- **Dezvoltarea sistemului de punctare pentru a permite o mai mare precizie.** De exemplu, ar putea fi introdus un procent de acoperire în locul răspunsului binar DA/NU pentru a ține mai bine seama de complexitatea consolidării capacităților la nivel național. Ca prim pas, a fost aleasă o abordare simplă cu răspunsuri DA/NU.
- **Introducerea unor indicatori cantitativi pentru a evalua eficacitatea SNSC a statelor membre.** Într-adevăr, cadrul de evaluare a capacităților naționale se axează pe evaluarea nivelului de maturitate al capacităților de securitate cibernetică ale statelor membre. Acesta ar putea fi completat de indicatori care să măsoare eficacitatea activităților și a planurilor de acțiune puse în aplicare de statele membre pentru a construi aceste capacități. Nu părea realist să se creeze astfel de indicatori de eficacitate în stadiul actual, având în vedere că: existau puține reacții din teren, era dificil să se identifice indicatori semnificativi care să coreleze realizările cu punerea în aplicare a SNSC și era dificil să se creeze indicatori realiști care să poată fi colectați ulterior. Acesta rămâne însă un subiect pentru lucrări viitoare.
- **Trecerea de la un exercițiu de autoevaluare la o abordare bazată pe evaluare.** O posibilă evoluție viitoare a cadrului ar putea fi trecerea la o abordare de evaluare pentru a evalua maturitatea capacităților de securitate cibernetică ale statelor membre într-un mod mai coerent. Efectuarea evaluării de către o parte terță ar putea, într-adevăr, să permită reducerea la minim a unei posibile părțialități.

ANEXA A – PREZENTARE GENERALĂ A REZULTATELOR CERCETĂRII DOCUMENTARE

Anexa A prezintă un rezumat al activității anterioare a ENISA cu privire la SNSC și o revizuire a modelelor de maturitate relevante disponibile public cu privire la capacitatea de securitate cibernetică. Pentru selectarea și revizuirea modelelor sunt luate în considerare următoarele ipoteze:

- nu toate modelele se bazează pe o metodologie de cercetare riguroasă;
- structura și rezultatele modelelor nu sunt întotdeauna explicate în detaliu, cu legături clare între diferitele elemente care caracterizează fiecare model;
- unele modele nu oferă detalii cu privire la procesul de dezvoltare, la structură și la metodologia de evaluare;
- alte modele și instrumente identificate nu oferă detalii cu privire la structură și conținut, drept pentru care nu sunt enumerate și
- selectarea modelelor de revizuire se bazează pe acoperirea geografică. Accentul principal va fi pus pe modelele de maturitate privind capacitățile de securitate cibernetică create pentru a evalua performanța țărilor europene. Cu toate acestea, este important să se extindă acoperirea geografică pentru a analiza bunele practici în ceea ce privește crearea unor modele de maturitate în întreaga lume.

Această revizuire sistematică a modelelor de maturitate relevante disponibile public privind capacitatea de securitate cibernetică a fost efectuată utilizând un cadru de analiză personalizat, bazat pe metodologia definită de Becker pentru dezvoltarea modelelor de maturitate[22]. Pentru fiecare model de maturitate existent au fost analizate următoarele elemente:

- **Denumirea modelului de maturitate:** Denumirea modelului de maturitate și referințele principale;
- **Instituția-sursă:** Instituția, fie publică sau privată, responsabilă de proiectarea modelului;
- **Scopul și obiectivul general:** Domeniul general de aplicare a modelului și obiectivul (obiectivele) vizat(e);
- **Numărul și definirea nivelurilor:** Numărul de niveluri de maturitate ale modelului, precum și descrierea generală a acestora;
- **Numărul și denumirea atributelor:** Numărul și denumirea atributelor utilizate de modelul de maturitate. Analiza atributelor are un obiectiv triplu:
  - defalcarea modelului de maturitate în secțiuni ușor de înțeles;
  - agregarea mai multor atribute în clustere de atribute care îndeplinesc același obiectiv și
  - prezentarea unor puncte de vedere diferite cu privire subiectul nivelului de maturitate.
- **Metodă de evaluare:** Metoda de evaluare a modelului de maturitate;
- **Reprezentarea rezultatelor**: Definirea metodei de vizualizare pentru rezultatele modelului de maturitate. Logica care stă la baza acestei etape este că modelele de maturitate tind să

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application" (Dezvoltarea modelelor de maturitate pentru gestionare IT: un model de procedură și aplicația sa), Business & Information Systems Engineering, vol. 1, nr. 3, pp. 213–222, iunie 2009.

eșueze dacă sunt prea complexe și, prin urmare, modul de reprezentare trebuie să răspundă nevoilor practice.

Activitățile anterioare cu privire la SNSC

ENISA a publicat două documente pe tema SNSC în 2012, ca parte a eforturilor sale timpurii. În primul rând, „Ghidul practic privind etapa de dezvoltare și realizare a SNSC”[23] a propus un set de acțiuni concrete pentru punerea în aplicare eficientă a unei SNSC și prezintă ciclul de viață al unei SNSC în patru etape: elaborarea strategiei, realizarea strategiei, evaluarea strategiei și menținerea strategiei. În al doilea rând, un document intitulat „Stabilirea cursului pentru eforturile naționale de consolidare a securității în spațiul cibernetic”[24] a prezentat stadiul strategiilor de securitate cibernetică în UE și în afara sa în 2012 și a propus ca statele membre să stabilească temele comune și diferențele dintre strategiile lor naționale de securitate cibernetică.

În 2014, a fost publicat primul cadru ENISA de evaluare a SNSC a unui stat membru[25]. Acest cadru conține recomandări și bune practici, precum și un set de instrumente de consolidare a capacităților pentru evaluarea unei SNSC (de exemplu, obiective identificate, intrări, ieșiri, indicatori-cheie de performanță etc.). Aceste instrumente sunt adaptate nevoilor diferite ale țărilor la diferite niveluri de maturitate în planificarea lor strategică. În același an, ENISA a publicat „Harta interactivă online a SNSC”[26], care permite utilizatorilor să consulte rapid SNSC ale tuturor statelor membre și țărilor AELS, inclusiv obiectivele lor strategice și bune exemple de punere în aplicare. Elaborată inițial ca registru al SNSC (2014), aceasta a fost actualizată cu exemple de punere în aplicare în 2018, iar începând din 2019 și până în prezent harta funcționează ca un *centru de informații* pentru centralizarea datelor furnizate de statele membre cu privire la eforturile lor de consolidare a securității cibernetice la nivel național.

Publicat în 2016, „Ghidul de bune practici privind SNSC”[27] identifică cincisprezece obiective strategice. De asemenea, acest ghid analizează stadiul punerii în aplicare a SNSC din fiecare stat membru și identifică diferite lacune și provocări în ceea ce privește punerea în aplicare.

În 2018, ENISA a publicat „Instrumentul de evaluare a strategiilor naționale de securitate cibernetică”[28]: un instrument interactiv de autoevaluare pentru a sprijini statele membre să își evalueze prioritățile strategice și obiectivele legate de SNSC. Prin intermediul unui set de întrebări simple, acest instrument oferă statelor membre recomandări specifice pentru punerea în aplicare a fiecărui obiectiv. În cele din urmă, documentul „Bunele practici în materie de inovare în domeniul securității cibernetice în cadrul SNSC”[29], publicat în 2019, prezintă subiectul inovării în domeniul securității cibernetice în cadrul SNSC. Documentul prezintă

[23] NCSS: Practical Guide on Development and Execution (SNSC: Ghid practic de dezvoltare și realizare) (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 (SNSC: Stabilirea cursului pentru eforturile naționale de consolidare a securității în spațiul cibernetic) (ENISA, 2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (Un cadru de evaluare pentru SNSC) (ENISA, 2014) https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (Strategiile naționale de securitate cibernetică – hartă interactivă) (ENISA, 2014, updated in 2019) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Prezentul document actualizează ghidul din 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Ghidul de bune practici privind SNSC: Conceperea și punerea în aplicare a strategiilor naționale de securitate cibernetică) (ENISA, 2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (Instrumentul de evaluare a strategiilor naționale de securitate cibernetică) (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

provocări și bune practici din diferitele dimensiuni ale inovării, astfel cum sunt percepute de experții în domeniu, pentru a contribui la elaborarea viitoarelor obiective strategice inovatoare.

A.1 Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM)

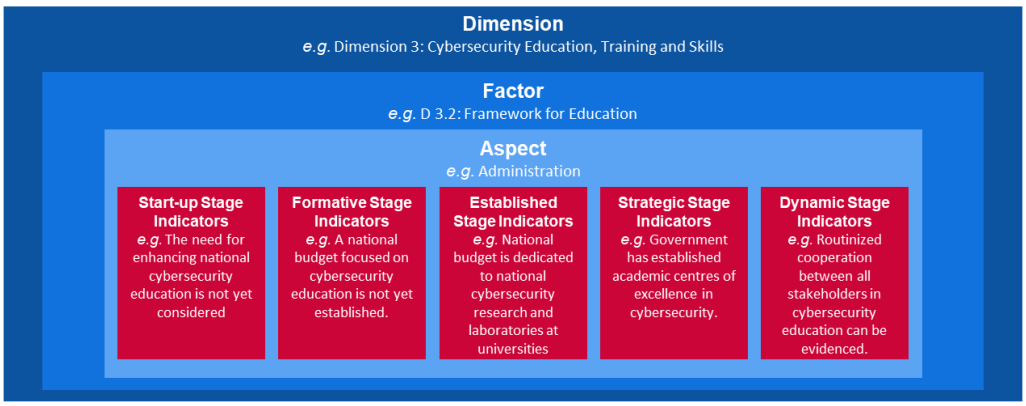
Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM) a fost elaborat de Global Cyber Security Capacity Centre (Centrul de capacități), care face parte din Școala Oxford Martin din cadrul Universității Oxford. Obiectivul Centrului de capacități este de a spori amploarea și eficacitatea consolidării capacităților în materie de securitate cibernetică, atât în Regatul Unit, cât și la nivel internațional, prin implementarea modelului de maturitate a capacităților de securitate cibernetică (CMM). CMM vizează în mod direct țările care doresc să își sporească capacitatea națională de securitate cibernetică. Aplicat inițial în 2014, CMM a fost revizuit în 2016 în urma utilizării sale în cadrul revizuirii a 11 capacități naționale de securitate cibernetică.

Atribute/Dimensiuni

În conformitate cu CMM, capacitatea de securitate cibernetică cuprinde **cinci dimensiuni** care reprezintă clusterele de capacitate de securitate cibernetică. Fiecare cluster reprezintă o perspectivă de cercetare diferită prin care capacitatea de securitate cibernetică poate fi studiată și înțeleasă. În cadrul celor cinci dimensiuni, **factorii** descriu detaliile deținerii capacității de securitate cibernetică. Aceste detalii sunt elemente care contribuie la îmbunătățirea maturității capacității de securitate cibernetică în cadrul fiecărei dimensiuni. Pentru fiecare factor, mai multe **aspecte** reprezintă componente diferite ale factorului. Aspectele reprezintă o metodă organizațională de împărțire a indicatorilor în clustere mai mici, care sunt mai ușor de înțeles. Fiecare aspect este evaluat ulterior pe baza unor **indicatori** pentru a descrie etapele, acțiunile sau componentele care indică o anumită etapă de maturitate (definită în secțiunea următoare) în cadrul unui aspect, al unui factor și al unei dimensiuni distincte.

Termenii sus-menționați pot fi stratificați, astfel cum se arată în figura de mai jos.

Figura 4: Exemple de indicatori CMM



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills

Dimensiunea
de exemplu, Dimensiunea 3: Educația, formarea și competențele în materie de securitate cibernetică

Factor
e.g. D 3.2: Framework for Education

Factor
de exemplu, D 3.2: Cadrul pentru educație

Aspect
e.g. Administration

Aspect
de exemplu, Administrație

Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indicatorii etapei inițiale, de exemplu educația pentru îmbunătățirea securității cibernetice naționale încă nu este luată în considerare
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indicatorii etapei formative, de exemplu un buget național axat pe educația în domeniul securității cibernetice încă nu este stabilit
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indicatori etapei stabilite, de exemplu bugetul național este dedicat cercetării și laboratoarelor în materie de securitate cibernetică națională din universități
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Pot fi puși în evidență indicatori ai etapei strategice; de exemplu, Guvernul a înființat un centru academic de excelență în educația în domeniul securității cibernetice.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicatori etapei dinamice; de exemplu, cooperare de rutină între toate părțile interesate

Cele cinci dimensiuni sunt detaliate mai jos:

i elaborarea unei politici și a unei strategii în materie de securitate cibernetică (6 factori);
ii încurajarea unei culturi responsabile în materie de securitate cibernetică în societate (5 factori);
iii dezvoltarea cunoștințelor în materie de securitate cibernetică (3 factori);
iv crearea unor cadre juridice și de reglementare eficace (3 factori) și
v controlul riscurilor prin standarde, organizații și tehnologii (7 factori).

Niveluri de maturitate

CMM utilizează **5 niveluri de maturitate** pentru a determina în ce măsură a progresat o țară în raport cu un anumit factor/aspect al capacității de securitate cibernetică. Aceste niveluri servesc drept imagini de ansamblu ale capacității existente în materie de securitate cibernetică:

- **Inițial**: în această etapă, fie nu există maturitate în materie de securitate cibernetică, fie aceasta este în stare embrionară. Ar putea exista discuții inițiale cu privire la consolidarea capacităților în materie de securitate cibernetică, dar nu au fost luate măsuri concrete. În această etapă nu există dovezi observabile;
- **Formativ**: unele caracteristici ale aspectelor au început să se dezvolte și să fie formulate, dar pot fi ad-hoc, dezorganizate, slab definite sau pur și simplu „noi”. Cu toate acestea, dovada acestei activități poate fi demonstrată în mod clar;
- **Stabilit**: elementele acestui aspect există și funcționează. Cu toate acestea, nu există o analiză bine gândită a alocării relative a resurselor. S-au luat puține decizii bazate pe compromis în ceea ce privește investițiile „relative” în diferitele elemente ale acestui aspect. Cu toate acestea, aspectul este funcțional și definit;
- **Strategic**: s-au făcut alegeri cu privire la părțile aspectului care sunt importante și care sunt mai puțin importante pentru organizația sau națiunea respectivă. Etapa strategică reflectă faptul că aceste alegeri au fost făcute, în funcție de circumstanțele specifice ale națiunii sau ale organizației și
- **Dinamic**: în această etapă, există mecanisme clare de modificare a strategiei în funcție de circumstanțele predominante, cum ar fi tehnologia mediului de amenințări, conflictul global sau o schimbare semnificativă într-un domeniu de interes (de exemplu, criminalitatea informatică sau protejarea vieții private). Organizațiile dinamice au elaborat metode de modificare a strategiilor. Procesul decizional rapid, realocarea resurselor și atenția constantă acordată mediului în schimbare sunt caracteristici ale acestei etape.

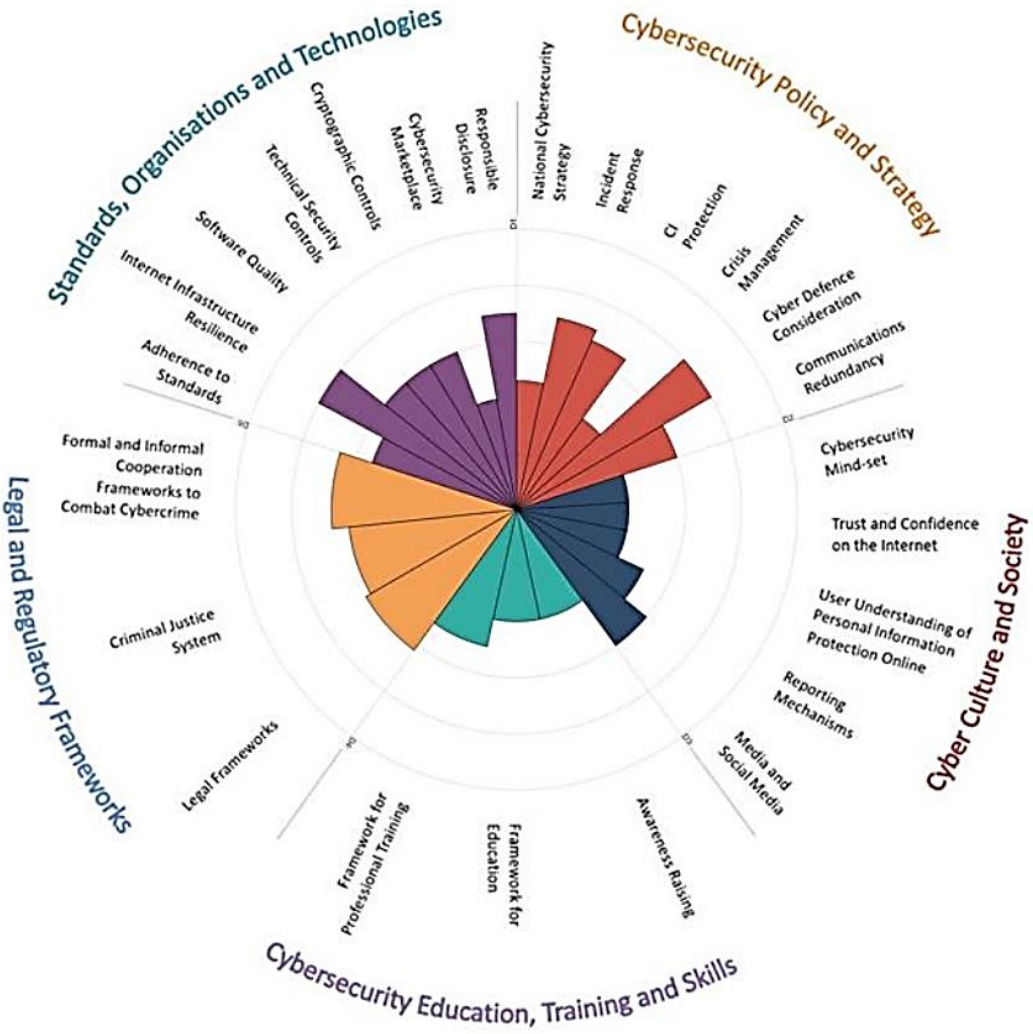
Metodă de evaluare

Întrucât Centrul de capacități nu are o înțelegere detaliată și aprofundată a fiecărui context intern în care este implementat modelul, acesta colaborează cu organizații internaționale, ministere sau organizații-gazdă din țara respectivă pentru a revizui maturitatea capacității de securitate cibernetică. Pentru a evalua nivelul de maturitate al celor cinci dimensiuni incluse în CMM, Centrul de capacități și organizația-gazdă se întâlnesc cu părțile interesate relevante de la nivel național din sectoarele public și privat pe parcursul a 2 sau 3 zile pentru a organiza grupuri de discuții asupra dimensiunilor CMM. Fiecare dimensiune este discutată cel puțin de două ori de către grupuri diferite de părți interesate. Aceasta constituie baza preliminară de date pentru evaluarea ulterioară.

Modul sau reprezentarea rezultatelor

CCM oferă o imagine de ansamblu asupra nivelului de maturitate al fiecărei țări prin intermediul unui radar compus din cinci secțiuni, câte una pentru fiecare dimensiune. Fiecare dimensiune reprezintă o cincime din grafic, cele cinci etape de maturitate pentru fiecare factor extinzându-se spre exterior dinspre centrul graficului; astfel cum se arată mai jos, etapa „inițială” este cea mai apropiată de centrul graficului, iar etapa „dinamică” se află pe perimetru exterior.

Figura 5 CMM: Prezentarea generală a rezultatelor



Standards, Organisations and Technologies
Legal Regulatory Frameworks

Standarde, organizații și tehnologii
Cadre juridice de reglementare

Cybersecurity Education, Training and Skills	Educația, formarea și competențele în materie de securitate cibernetică
Cybersecurity Policy and Strategy	Politica și strategia în materie de securitate cibernetică
Cyber Culture and Society	Cultura și societatea cibernetică
Responsible Disclosure	Divulgare responsabilă
Cybersecurity market place	Piața securității cibernetice
Cryptographic Controls	Controale criptografice
Technical Security Controls	Controale tehnice de securitate
Software Quality	Calitatea software-ului
Internet Infrastructure Resilience	Reziliența infrastructurii de internet
Adherence to Standards	Aderarea la standarde
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Cadre de cooperare formale și informale pentru combaterea criminalității informatice
Criminal Justice System	Sistemul de justiție penală
Legal Frameworks	Cadre juridice
Framework for Professional Training	Cadrul pentru formarea profesională
Framework for Education	Cadrul pentru educație
Awareness Raising	Sensibilizare
Media and Social Medai	Mass-media și platformele de comunicare socială
Reporting Mechanisms	Mecanisme de raportare
User Understanding of Personal Information Protection Online	Înțelegerea utilizatorilor cu privire la protecția informațiilor cu caracter personal online
Trust and Confidence on the Internet	Încredere și încredere pe internet
Cybersecurity Mind-set	Mentalitate orientată spre securitate cibernetică
Communications Redundancy	Redundanță în materie de comunicare
Cyber Defence Consideration	Considerații privind apărarea cibernetică
Crisis Management	Gestionarea crizelor
CI Protection	Protecția CI
Incident Response	Răspunsul la incidente
National Cybersecurity Strategy	Strategia națională de securitate cibernetică

Global Cyber Security Capacity Centre Oxford Martin School, Universitatea Oxford, 2017.

A.2 Modelul de maturitate a capacității de securitate cibernetică (C2M2)

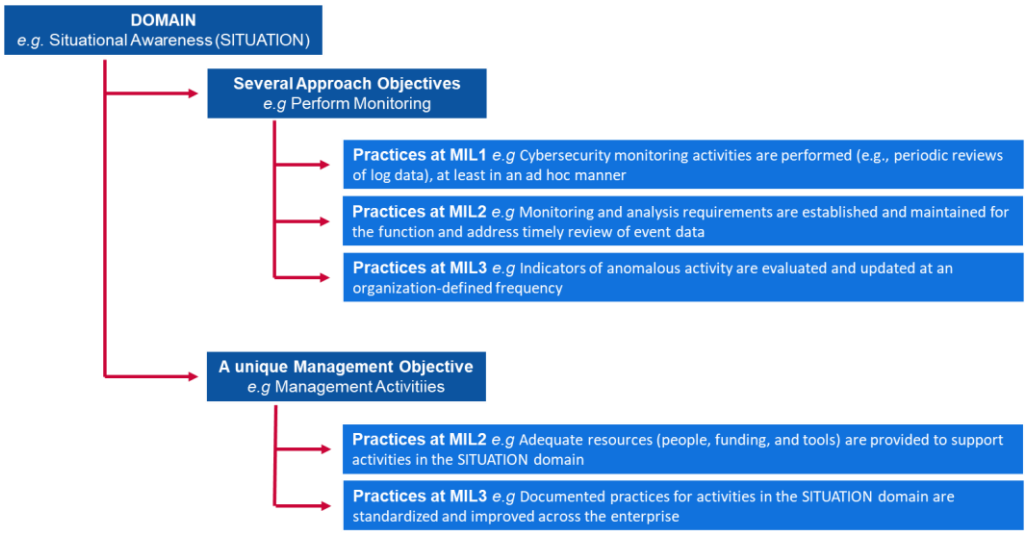
Modelul de maturitate a capacității de securitate cibernetică (C2M2) a fost elaborat de Departamentul pentru Energie al SUA în colaborare cu experți din sectorul public și privat. Obiectivul Centrului de capacități este de a ajuta organizațiile din toate sectoarele, de toate tipurile și de toate dimensiunile să evalueze și să îmbunătățească programele lor de securitate cibernetică și să își consolideze reziliența operațională. C2M2 se axează pe punerea în aplicare și gestionarea practicilor în materie de securitate cibernetică asociate cu activele din domeniul informațiilor, al tehnologiei informației (TI) și a tehnologiei de operare (OT) și cu mediile în care acestea funcționează. C2M2 definește modelele de maturitate ca fiind: „un set de caracteristici, atribute, indicatori sau modele care reprezintă capacitatea și evoluția într-o anumită disciplină”. Lansat inițial în 2014, C2M2 a fost revizuit în 2019.

Atribute/Dimensiuni

C2M2 ia în considerare **zece domenii** care reprezintă o grupare logică a practicilor în materie de securitate cibernetică. Fiecare set de practici reprezintă activitățile pe care le poate desfășura o organizație pentru a stabili și a dezvolta capacități în domeniu. Fiecare domeniu este asociat ulterior cu un **obiectiv unic de gestionare** și cu **mai multe obiective de abordare**. Atât în cadrul obiectivelor de abordare, cât și în cel al obiectivelor de gestionare sunt detaliate **mai multe practici** pentru a descrie activitățile instituționalizate.

Relația dintre aceste noțiuni este rezumată mai jos:

Figura 6: Exemplu de indicator C2M2



Domain eg Situational Awareness (SITUATION)	**Domeniu,** de exemplu conștientizarea situației (SITUAȚIE)
Several Approaches Objectives e.g. Perform Monitoring	**Mai multe obiective de abordare,** de exemplu monitorizarea performanței
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Practici la MIL1**, de exemplu activități de monitorizare a securității cibernetice (cum ar fi revizuiri periodice ale datelor din registre), cel puțin în mod ad-hoc
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Practici la MIL2**, de exemplu cerințele de monitorizare și analiză sunt stabilite și menținute pentru funcția și abordarea revizuirii în timp util a datelor incidentelor
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Practici la MIL3,** de exemplu indicatorii activității anormale sunt evaluați și actualizați cu o frecvență definită de organizație
A unique Management Objectve e.g. Management Activities	Un obiectiv unic de gestionare, de exemplu activitățile de gestionare
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Practici la MIL2,** de exemplu sunt puse la dispoziție resurse adecvate (persoane, finanțare și instrumente) pentru a sprijini activitățile din domeniul SITUAȚIE
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Practici la MIL3,** de exemplu practicile documentate pentru activitățile din domeniul SITUAȚIE sunt standardizate și îmbunătățite la nivelul întreprinderii

Cele zece domenii sunt detaliate mai jos:

i Gestionarea riscurilor (RISC);
ii Gestionarea activelor, a modificărilor și a configurației (ACTIVE);
iii Gestionarea identității și a accesului (ACCES);
iv Gestionarea amenințărilor și a vulnerabilităților (AMENINȚARE);
v Conștientizarea situației (SITUAȚIE);
vi Răspunsul la incidente și evenimente (RĂSPUNS);
vii Gestionarea lanțului de aprovizionare și a dependențelor externe (DEPENDENȚE);
viii Gestionarea forței de muncă (FORȚA DE MUNCĂ);
ix Arhitectura de securitate cibernetică (ARHITECTURĂ) și
x Gestionarea programului de securitate cibernetică (PROGRAM).

Niveluri de maturitate

C2M2 utilizează **4 niveluri de maturitate** [denumite niveluri ale indicatorului de maturitate (Maturity Indicator Levels – MIL)] pentru a determina o dublă evoluție a maturității: o evoluție a abordării și o evoluție a gestionării. Valorile MIL variază de la MIL0 la MIL3 și sunt concepute pentru a fi aplicate independent în fiecare domeniu.

- **MIL0**: Practicile nu sunt aplicate.
- **MIL1**: Practicile inițiale sunt aplicate, dar pot fi ad-hoc.
- **MIL2**: Caracteristici de gestionare:

- practicile sunt documentate;
- sunt puse la dispoziție resurse adecvate pentru a sprijini procesul;
- personalul care aplică practicile are competențe și cunoștințe adecvate și
- se atribuie responsabilitatea și autoritatea pentru punerea în aplicare a practicilor.

Caracteristici de abordare:

- practicile sunt mai complete sau mai avansate decât la MIL1.

- **MIL3**: Caracteristici de gestionare:
  - activitățile sunt ghidate de politici (sau de alte directive organizaționale);
  - obiectivele de performanță pentru activitățile din domeniu sunt stabilite și monitorizate pentru a urmări rezultatele obținute și
  - practicile documentate pentru activitățile din domeniu sunt standardizate și îmbunătățite la nivelul întreprinderii.

  Caracteristici de abordare:
  - practicile sunt mai complete sau mai avansate decât la MIL2.

Metodă de evaluare

C2M2 este conceput pentru a fi utilizat împreună cu un set de instrumente și o **methodologie de autoevaluare** (disponibile la cerere) pentru ca o organizație să își evalueze și să își îmbunătățească programul de securitate cibernetică. O autoevaluare cu ajutorul setului de instrumente poate fi finalizată într-o singură zi, dar setul de instrumente ar putea fi adaptat pentru un efort de evaluare mai riguros. În plus, C2M2 poate fi utilizat pentru a orienta dezvoltarea unui nou program de securitate cibernetică.

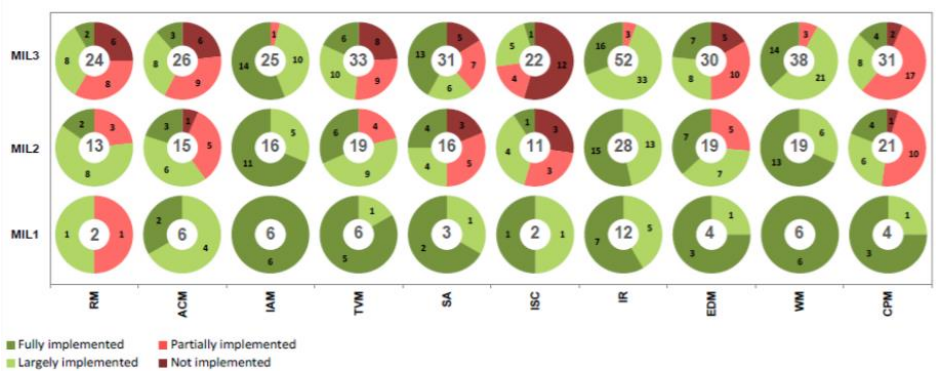
Conținutul modelului este prezentat la un nivel ridicat de abstracție, astfel încât să poată fi interpretat de organizații de diferite tipuri, structuri, dimensiuni și industrii. Utilizarea pe scară largă a modelului de către un sector poate sprijini evaluarea comparativă a capacităților de securitate cibernetică ale sectorului.

Modul sau reprezentarea rezultatelor

C2M2 oferă un raport de punctare de evaluare întocmit pe baza rezultatelor sondajului. Raportul prezintă rezultatele în două imagini: imaginea Obiective, care prezintă răspunsurile practice la întrebări pentru fiecare domeniu și de obiectivele acestuia, și imaginea Domeniu, care prezintă răspunsuri pentru toate domeniile și valorile MIL. Ambele imagini se bazează pe un sistem de reprezentare caracterizat prin diagrame inelare, una per răspuns, și un mecanism de punctare de tip semafor. Astfel cum se arată în Figura 7, sectoarele roșii dintr-o diagramă inelară arată numărul de întrebări care au primit răspunsuri de tip „neaplicate” (roșu închis) sau „aplicate parțial” (roșu deschis). Sectoarele verzi prezintă numărul de întrebări care au primit răspunsuri tip „aplicate pe scară largă” (verde deschis) sau „aplicate integral” (verde închis).

În Figura 7 de mai jos este prezentat un exemplu de card de punctare la sfârșitul unei evaluări a maturității. În axa X sunt cele 10 domenii ale C2M2, iar în axa Y, nivelurile de maturitate (MIL). Analizând graficul și luând în considerare domeniul gestionării riscurilor (RM), este posibilă observarea a trei diagrame inelare, câte una corespunzătoare fiecărui nivel de maturitate MIL1, MIL2 și MIL3. Pentru domeniul RM, graficul evidențiază faptul că există două elemente care trebuie evaluate pentru atingerea primului nivel de maturitate, MIL1. În acest caz, un calificativ „aplicate în mare măsură” și un calificativ „aplicate parțial”. Pentru al doilea nivel de maturitate, MIL2, modelul prevede 13 elemente care urmează să fie evaluate. Două dintre aceste 13 elemente aparțin primului nivel, MIL1, iar 11 celui de al doilea nivel, MIL2. Același lucru este valabil pentru al treilea nivel, MIL3.

Figura 7: C2M2 – Exemplu de imagine Domeniu



Fully implemented	Aplicate integral
Largely implemented	Aplicate pe scară largă
Partially implemented	Aplicate parțial
Not implemented	Neaplicate
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Sursa: Departamentul pentru Energie al SUA, Office of electricity delivery and energy reliability (Biroul pentru furnizarea de energie electrică și fiabilitatea energetică), 2015.

A.3 Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice

Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice a fost elaborat în cadrul Institutului Național de Standarde și Tehnologie (NIST). Acesta se concentrează pe orientarea activităților legate de securitatea cibernetică și pe gestionarea riscurilor în cadrul unei organizații. Acesta vizează toate tipurile de organizații, indiferent de dimensiune, de gradul de risc de securitate cibernetică sau de sofisticarea în materie de securitate cibernetică. Deoarece este un cadru și nu un model, acesta este creat diferit față de modelele analizate anterior.

Cadrul este alcătuit din trei părți: cadrul de bază, nivelurile de aplicare și profilurile de cadru:

- **Cadrul de bază** reprezintă un set de activități legate de securitatea cibernetică, rezultate dorite și referințe aplicabile care sunt comune în toate sectoarele cu infrastructuri critice. Acestea sunt similare atributelor sau dimensiunilor identificate în modelele de maturitate a capacității de securitate cibernetică.
- **Nivelurile de aplicare a cadrului** („nivelurile”) oferă un context cu privire la modul în care o organizație percepe riscul de securitate cibernetică și procesele instituite pentru gestionarea riscului respectiv. De la parțial (nivelul 1) la adaptabil (nivelul 4), nivelurile descriu un grad din ce în ce mai mare de rigurozitate și complexitate în practicile de gestionare a riscurilor pentru securitatea cibernetică. Nivelurile nu reprezintă niveluri de maturitate, ci au scopul de a sprijini procesul decizional organizațional cu privire la modul de gestionare a riscurilor pentru securitatea cibernetică, precum și la

dimensiunile organizației care au o prioritate mai mare și ar putea primi resurse suplimentare.

- Un **profil de cadru** („profil") reprezintă rezultatele bazate pe nevoile operaționale pe care o organizație le-a selectat din categoriile și subcategoriile cadrului. Profilul poate fi caracterizat în ceea ce privește alinierea standardelor, a orientărilor și a practicilor la cadrul de bază într-un anumit scenariu de punere în aplicare. Profilurile pot fi utilizate pentru a identifica posibilitățile de îmbunătățire a poziției în materie de securitate cibernetică prin compararea unui profil „actual" (starea „ca atare") cu un profil „țintă" (starea „vizată").

Cadrul de bază

Cadrul de bază cuprinde cinci **funcții**. Atunci când sunt analizate împreună, aceste funcții oferă o viziune strategică de înalt nivel a ciclului de viață al gestionării riscului de securitate cibernetică de către o organizație. Cadrul de bază identifică ulterior **categorii**-cheie și **subcategorii** pentru fiecare funcție și le asociază cu exemple de referințe informative, cum ar fi standardele, orientările și practicile existente pentru fiecare subcategorie.

Funcțiile și categoriile sunt detaliate mai jos:

i **Identificare**: Dezvoltarea unei înțelegeri organizaționale a modului de gestionare a riscurilor de securitate cibernetică pentru sisteme, persoane, active, date și capacități.
- Subcategorii: Gestionarea activelor, Mediul de afaceri, Guvernanță, Evaluarea riscurilor și Strategia de gestionare a riscurilor

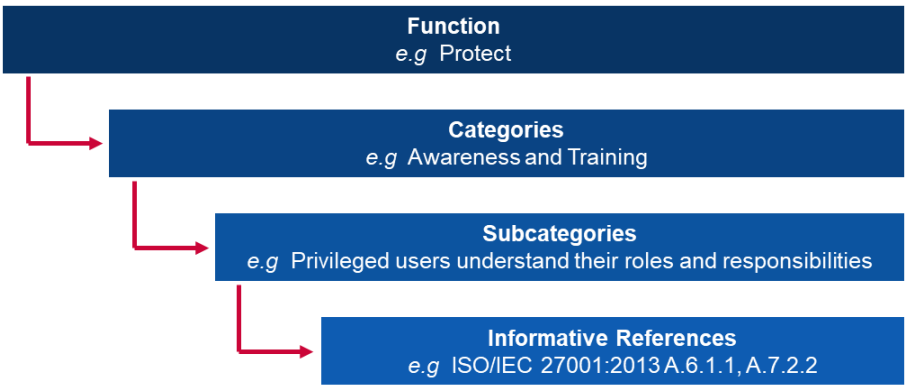
ii **Protejare**: Elaborarea și punerea în aplicare a unor garanții adecvate pentru a asigura furnizarea de servicii critice.
- Subcategorii: Gestionarea identității și controlul accesului, Sensibilizare și formare, Securitatea datelor, Procesele și procedurile de protecție a informațiilor, Întreținerea și Tehnologia de protecție

iii **Detectare**: Elaborarea și punerea în aplicare a unor activități adecvate pentru a identifica producerea unui eveniment de securitate cibernetică.
- Subcategorii: Anomalii și evenimente, Monitorizarea continuă a securității și Procesele de detectare.

iv **Răspuns**: Elaborarea și punerea în aplicare a unor activități adecvate pentru a lua măsuri cu privire la un incident de securitate cibernetică detectat.
- Subcategorii: Planificarea răspunsului, Comunicații, Analiză, Atenuare și Îmbunătățiri.

v **Recuperare**: Elaborarea și punerea în aplicare a unor activități adecvate pentru a menține planuri de reziliență și pentru a restabili capabilitățile sau serviciile care au fost afectate de un incident de securitate cibernetică.
- Subcategorii: Planificarea redresării, Îmbunătățiri și Comunicații

Figura 8: Exemplu de cadru pentru îmbunătățirea securității cibernetice a infrastructurilor critice



Function e.g Project
Categories e.g Awarness and Training

Funcție, de exemplu Proiect
Categorii, de exemplu Sensibilizare și formare

Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Subcategorii, de exemplu Utilizatori privilegiați care își înțeleg rolurile și responsabilitățile
Referințe informative, de exemplu ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Niveluri

Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice se bazează pe **4 niveluri**, fiecare dintre acestea fiind definit de-a lungul a trei axe: procesul de gestionare a riscurilor, programul integrat de gestionare a riscurilor și participarea externă. Nivelurile nu trebuie considerate niveluri de maturitate, ci un cadru care le oferă organizațiilor o contextualizare a opiniilor lor cu privire la riscul de securitate cibernetică și la procesele instituite pentru gestionarea riscului respectiv.

- **Nivelul 1: Parțial**
  - **Procesul de gestionare a riscurilor**: practicile organizaționale de gestionare a riscurilor de securitate cibernetică nu sunt formalizate, iar riscul este gestionat în mod ad-hoc și uneori reactiv;
  - **Programul integrat de gestionare a riscurilor**: conștientizarea riscului de securitate cibernetică la nivel organizațional este limitată. Organizația pune în aplicare gestionarea riscurilor de securitate cibernetică în mod neregulat, de la caz la caz, și este posibil să nu dispună de procese care să permită partajarea informațiilor privind securitatea cibernetică în cadrul organizației;
  - **Participare externă**: organizația nu înțelege rolul său în ecosistemul mai larg nici în ceea ce privește dependențele sale, nici în ceea ce privește persoanele dependente. În general, organizația nu cunoaște riscurile lanțului de aprovizionare din domeniul cibernetic ale produselor și serviciilor pe care le furnizează și pe care le utilizează;
- **Nivelul 2: Risc informat**
  - **Procesul de gestionare a riscurilor**: practicile de gestionare a riscurilor sunt aprobate de conducere, dar nu pot fi stabilite ca o politică la nivel organizațional;
  - **Programul integrat de gestionare a riscurilor**: se conștientizează riscurile în materie de securitate cibernetică la nivel organizațional, dar nu a fost stabilită o abordare la nivelul întregii organizații în ceea ce privește gestionarea riscurilor de securitate cibernetică. Evaluarea riscurilor cibernetice ale activelor organizaționale și externe este efectuată, dar nu este, de regulă, repetabilă sau periodică;
  - **Participare externă**: în general, organizația își înțelege rolul în ecosistemul mai larg în ceea ce privește fie propriile dependențe, fie persoanele dependente, dar nu ambele. În plus, organizația este conștientă de riscurile lanțului de aprovizionare în domeniul cibernetic asociate produselor și serviciilor pe care le furnizează și le utilizează, dar nu acționează în mod consecvent sau formal cu privire la aceste riscuri;
- **Nivelul 3: Repetabil**
  - **Procesul de gestionare a riscurilor**: practicile de gestionare a riscurilor ale organizației sunt aprobate oficial și exprimate ca politică. Practicile organizaționale în materie de securitate cibernetică sunt actualizate periodic pe baza aplicării proceselor de gestionare a riscurilor la modificările cerințelor privind activitățile/misiunile și a unei situații tehnologice și a amenințărilor în schimbare;
  - **Programul integrat de gestionare a riscurilor**: există o abordare la nivelul întregii organizații pentru gestionarea riscurilor de securitate cibernetică. Politicile, procesele și procedurile bazate pe cunoașterea riscurilor sunt definite, puse în aplicare în modul prevăzut și revizuite. Cadrele superioare de conducere asigură luarea în considerare a securității cibernetice prin toate liniile operaționale din cadrul organizației;
  - **Participare externă**: organizația își înțelege rolul, dependențele și persoanele dependente din ecosistemul mai larg și poate contribui la înțelegerea mai aprofundată a riscurilor de către comunitate. Organizația este conștientă de riscurile lanțului de aprovizionare din domeniul cibernetic asociate produselor și serviciilor pe care le furnizează și pe care le utilizează;

- **Nivelul 4: Adaptativ**
  - **Procesul de gestionare a riscurilor**: organizația își adaptează practicile în materie de securitate cibernetică pe baza activităților anterioare și actuale legate de securitatea cibernetică, inclusiv a lecțiilor învățate și a indicatorilor predictivi;
  - **Programul integrat de gestionare a riscurilor**: există o abordare la nivelul întregii organizații în ceea ce privește gestionarea riscurilor de securitate cibernetică, care utilizează politici, procese și proceduri bazate pe cunoașterea riscurilor pentru a aborda eventualele evenimente în domeniul securității cibernetice și
  - **Participare externă**: organizația își înțelege rolul, dependențele și persoanele dependente din ecosistemul mai larg și contribuie la înțelegerea mai aprofundată a riscurilor de către comunitate.

Metodă de evaluare

Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice este menit să le permită organizațiilor să își autoevalueze riscurile pentru ca abordarea și investițiile lor în materie de securitate cibernetică să devină mai raționale, mai eficace și mai valoroase. Pentru a examina eficacitatea investițiilor, o organizație trebuie să aibă mai întâi o înțelegere clară a obiectivelor sale organizaționale, a relației dintre aceste obiective și a rezultatelor de sprijin în materie de securitate cibernetică. Rezultatele în materie de securitate cibernetică ale cadrului de bază sprijină autoevaluarea eficacității investițiilor și a activităților legate de securitatea cibernetică.

A.4 Modelul de maturitate a capacității de securitate cibernetică al Qatarului (Q-C2M2)

Modelul de maturitate a capacității de securitate cibernetică al Qatarului (Q-C2M2) a fost elaborat în 2018 de Colegiul de Drept al Universității Qatar. Q-C2M2 se bazează pe diferite modele existente pentru a elabora o metodologie cuprinzătoare de evaluare pentru a consolida cadrul de securitate cibernetică al Qatarului.

Atribute/Dimensiuni

Q-C2M2 adoptă abordarea Cadrului Institutului Național de Standarde și Tehnologie (NIST) de a utiliza cinci funcții de bază ca domenii principale ale modelului. Cele cinci funcții principale sunt aplicabile în contextul Qatarului deoarece sunt comune în toate sectoarele infrastructurii critice, un element important al cadrului de securitate cibernetică al Qatarului. Q-C2M2 se bazează pe **cinci domenii**, fiecare domeniu fiind împărțit ulterior în mai multe **subdomenii** pentru a acoperi întreaga gamă de maturitate a capacităților de securitate cibernetică.

Cele cinci domenii sunt detaliate mai jos:

i **Domeniul Înțelegere** include patru subdomenii: guvernanța cibernetică, activele, riscurile și formarea;
ii subdomeniile din **domeniul Securitizare** includ securitatea datelor, securitatea tehnologică, securitatea controlului accesului, securitatea comunicațiilor și securitatea personalului;
iii **Domeniul Expunere** include subdomeniile: monitorizare, gestionarea incidentelor, detectare, analiză și expunere;
iv **Domeniul Răspuns** include planificarea răspunsului, atenuarea și comunicarea răspunsului și
v **Domeniul Susținere** include planificarea redresării, gestionarea continuității, îmbunătățire și dependențe externe.

Niveluri de maturitate

Q-C2M2 utilizează **5 niveluri de maturitate** care măsoară maturitatea capacității unei entități de stat sau a unei organizații nestatale la nivelul funcției de bază. Aceste niveluri vizează evaluarea maturității în cele cinci domenii detaliate în secțiunea anterioară.

- **Inițiere**: se utilizează practici și procese ad-hoc în materie de securitate cibernetică în unele domenii;
- **Aplicare**: s-au adoptat politici de punere în aplicare a tuturor activităților legate de securitatea cibernetică din domeniile respective, cu scopul de a finaliza punerea în aplicare la un anumit moment;
- **Dezvoltare**: s-au pus în aplicare politici și practici pentru dezvoltarea și îmbunătățirea activităților legate de securitatea cibernetică din domeniile respective, cu scopul de a sugera noi activități care să fie puse în aplicare;
- **Adaptabil**: se reexaminează și se revizuiesc activitățile legate de securitatea cibernetică și se adoptă practici bazate pe indicatori predictivi derivați din experiențele și măsurile anterioare și
- **Agil**: se practică în continuare etapa adaptabilă, punând un accent sporit pe agilitate și viteză în punerea în aplicare a activităților în domenii.

Metodă de evaluare

Q-C2M2 se află într-un stadiu incipient al cercetării și nu este încă construit pentru a fi pus în aplicare. Acesta este un cadru care ar putea fi utilizat pentru a implementa în viitor un model detaliat de evaluare pentru organizațiile din Qatar.

A.5 Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)

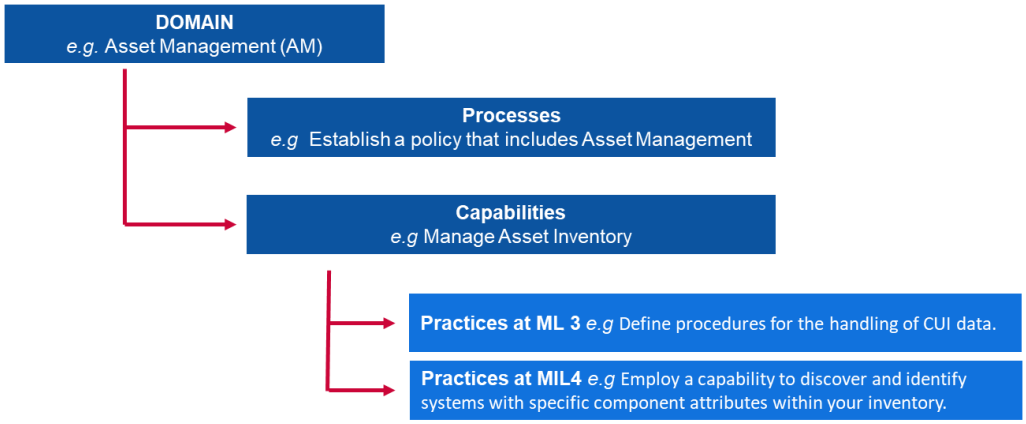
Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC) a fost elaborată de Departamentul de Apărare al SUA (DoD) în colaborare cu Universitatea Carnegie Mellon și cu Laboratorul de fizică aplicată al Universității Johns Hopkins. Principalul obiectiv al DoD în conceperea acestui model este de a proteja informațiile din sectorul bazei industriale de apărare (DIB). Informațiile vizate de CMMC sunt clasificate fie ca „informații privind contractele federale”, fie ca informații furnizate de guvern sau generate pentru acesta în temeiul unui contract care nu sunt destinate publicării, fie ca „informații neclasificate controlate”, informații care necesită controale de salvgardare sau diseminare în conformitate cu actele cu putere de lege, normele administrative și politicile la nivel guvernamental. CMMC evaluează maturitatea securității cibernetice și prevede cele mai bune practici, împreună cu un element de certificare, pentru a asigura punerea în aplicare a practicilor asociate fiecărui nivel de maturitate. Cea mai recentă versiune a CMMC a fost publicată în 2020.

Atribute/Dimensiuni

CMMC ia în considerare **șaptesprezece domenii** care reprezintă clustere de procese și capacități în materie de securitate cibernetică. Fiecare domeniu este defalcat ulterior în mai multe **procese** care sunt similare în toate domeniile; și în una sau mai multe **capacități** care acoperă cinci niveluri de maturitate. Capacitățile (sau capacitatea) sunt detaliate în continuare în **practici** pentru fiecare nivel de maturitate relevant.

Relația dintre aceste noțiuni este următoarea:

Figura 9: Exemple de indicatori CMMC



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data

Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

DOMENIU, de exemplu Gestionarea activelor (AM)
Procese
de exemplu stabilirea unei politici care să includă Gestionarea activelor
Capacități
de exemplu Gestionarea inventarului de active
Practici la MIL 3, de exemplu Definirea de proceduri pentru prelucrarea datelor CUI (informații neclasificate controlate)
Practici la MIL4, de exemplu Utilizarea unei capacități de a descoperi și de a identifica sisteme cu atribute specifice ale componentelor în cadrul inventarului

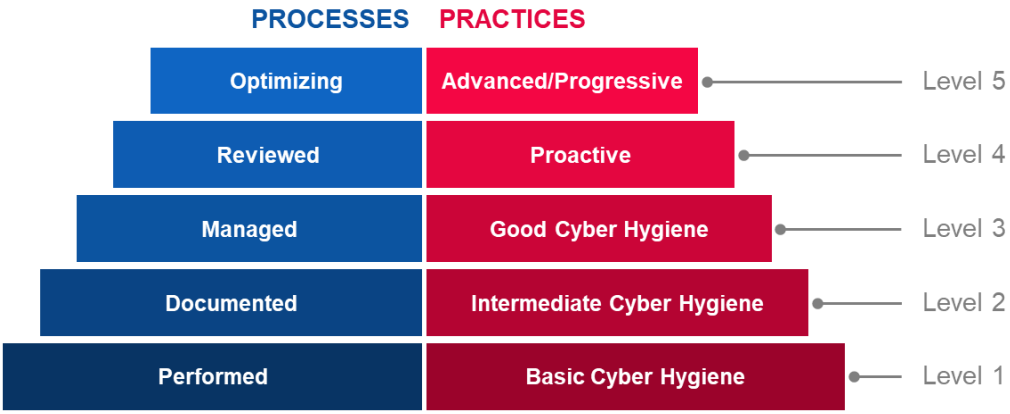
Cele șaptesprezece domenii sunt detaliate mai jos:

i controlul accesului (AC);
ii gestionarea activelor (AM);
iii audit și responsabilitate (AU);
iv sensibilizare și formare (AT);
v gestionarea configurației (CM);
vi identificare și autentificare (IA);
vii răspunsul în caz de incident (IR);
viii întreținere (MA);
ix protecția mass-mediei (MP);
x securitatea personalului (PS);
xi protecție fizică (PE);
xii redresare (RE);
xiii gestionarea riscurilor (RM);
xiv evaluarea securității (CA);
xv conștientizarea situației (SA);
xvi protecția sistemelor și comunicațiilor (CS) și
xvii integritatea sistemelor și a informațiilor (SI).

Niveluri de maturitate

CMMC utilizează **5 niveluri de maturitate** definite pe baza proceselor și practicilor. Pentru a atinge un anumit nivel de maturitate în CMMC, o organizație trebuie să îndeplinească condițiile prealabile pentru procesele și practicile pentru nivelul respectiv. Aceasta implică, de asemenea, îndeplinirea condițiilor prealabile pentru toate nivelurile situate sub nivelul respectiv.

Figura 10: Niveluri de maturitate CMMC



PROCESSES	PROCESE
Optimizing	Optimizare
Reviewed	Revizuite
Managed	Gestionate
Documented	Documentate
Performed	Realizate
PRACTICES	PRACTICI
Advanced/Progressive	Avansate/progresiste
Proactive	Proactive
Good Cyber Hygiene	O bună igienă cibernetică
Intermediate Cyber Hygiene	Igienă cibernetică intermediară
Basic Cyber Hygiene	Igienă cibernetică de bază
Level 5	Nivelul 5
Level 4	Nivelul 4
Level 3	Nivelul 3
Level 2	Nivelul 2
Level 1	Nivelul 1

- **Nivelul 1**
  - **Procese – Realizate**: deoarece organizația poate să aplice aceste practici doar ad-hoc și se poate baza sau nu pe documentație. Maturitatea procesului nu este evaluată pentru nivelul 1;
  - **Practici – Igienă cibernetică de bază**: nivelul 1 se axează pe protecția FCI (informații contractuale federale) și constă numai în practici care corespund cerințelor de bază în materie de protecție;
- **Nivelul 2**
  - **Procese – Documentate**: nivelul 2 impune ca o organizație să stabilească și să documenteze practici și politici care să ghideze punerea în aplicare a eforturilor sale în materie de CMMC. Documentarea practicilor permite persoanelor să le efectueze în mod repetabil. Organizațiile își dezvoltă capacități mature prin documentarea proceselor lor și apoi le practică astfel cum au fost documentate;
  - **Practici – Igienă cibernetică intermediară**: nivelul 2 servește drept evoluție de la nivelul 1 la nivelul 3 și constă într-un subset de cerințe de securitate specificate în NIST SP 800-171, precum și practici din alte standarde și referințe;
- **Nivelul 3**
  - **Procese – Gestionate**: nivelul 3 impune ca o organizație să elaboreze, să mențină și să pună la dispoziție un plan care să demonstreze gestionarea activităților pentru punerea în aplicare a practicilor. Planul poate include informații privind misiunile, obiectivele, planurile de proiect, resursele, formarea necesară și implicarea părților interesate relevante;
  - **Practici – O bună igienă cibernetică**: nivelul 3 se axează pe protecția CUI și cuprinde toate cerințele de securitate specificate în NIST SP 800-171, precum și

practici suplimentare față de alte standarde și referințe pentru atenuarea amenințărilor;

- **Nivelul 4**
  - **Procese – Revizuite**: nivelul 4 impune ca o organizație să analizeze și să evalueze practicile din punct de vedere al eficacității. Pe lângă practicile de evaluare a eficacității, organizațiile de la acest nivel sunt în măsură să ia măsuri corective atunci când este necesar și să informeze în mod recurent conducerea de nivel superior cu privire la statut sau probleme;
  - **Practici – Proactive**: nivelul 4 se axează pe protecția CUI (informații neclasificate controlate) și cuprinde un subset al cerințelor de securitate consolidate. Aceste practici sporesc capacitățile de detectare și de răspuns ale unei organizații pentru a aborda și a se adapta la tactica, tehnicile și procedurile în schimbare;
- **Nivelul 5**
  - **Procese – Optimizare**: nivelul 5 necesită ca o organizație să standardizeze și să optimizeze punerea în aplicare a proceselor în întreaga organizație și
  - **Practici – Avansate/Proactive**: nivelul 5 se axează pe protecția CUI. Practicile suplimentare sporesc profunzimea și complexitatea capacităților de securitate cibernetică.

Metodă de evaluare

CMMC este un model relativ nou, finalizat în primul trimestru al anului 2020. Până în prezent, CMMC nu a fost implementat în cadrul niciunei organizații. Cu toate acestea, contractanții DoD se așteaptă să contacteze examinatori terți certificați pentru efectuarea de audituri. DoD se așteaptă ca acești contractanți să pună în aplicare cele mai bune practici pentru a promova securitatea cibernetică și protecția informațiilor sensibile.

A.6 Modelul comunitar de maturitate în materie de securitate cibernetică (CCSMM)

Modelul comunitar de maturitate în materie de securitate cibernetică (CCSMM) a fost elaborat de Centrul pentru asigurarea infrastructurii și securitate din cadrul Universității Texas. Obiectivul CCSMM este de a defini mai bine metodele de determinare a statutului actual al unei comunități în ceea ce privește pregătirea sa în domeniul cibernetic și de a oferi o foaie de parcurs pentru comunități pe care acestea să o urmeze în eforturile lor de pregătire. Comunitățile vizate de CCSMM sunt în principal autoritățile locale sau guvernamentale. CCSMM a fost conceput în 2007.

Atribute/Dimensiuni

Nivelurile de maturitate sunt definite pe baza a **6 dimensiuni principale** care acoperă diferitele aspecte ale securității cibernetice în cadrul comunităților și al organizațiilor. Aceste dimensiuni sunt clar definite pentru fiecare nivel de maturitate (detaliate în Figura 31: Rezumatul dimensiunilor CCSMM) Cele 6 dimensiuni sunt:

i amenințări abordate;
ii indicatori;
iii schimb de informații;
iv tehnologie;
v formare și
vi test.

Niveluri de maturitate

CCSMM se întemeiază pe **5 niveluri de maturitate**, pe baza principalelor tipuri de amenințări și activități abordate la nivelul respectiv:

- **Nivelul 1: Sensibilizare cu privire la securitate**
  Principala temă a activităților la acest nivel este de a sensibiliza persoanele și

organizațiile cu privire la amenințările, problemele și aspectele legate de securitatea cibernetică;

- **Nivelul 2: Dezvoltarea proceselor**
  Nivelul conceput pentru a ajuta comunitățile să instituie și să îmbunătățească procesele de securitate necesare în scopul de a aborda în mod eficace aspectele legate de securitatea cibernetică;
- **Nivelul 3: Bazat pe informații**
  Conceput pentru a îmbunătăți mecanismele de schimb de informații în cadrul comunității în scopul de a permite comunității să coreleze efectiv informații aparent disparate.
- **Nivelul 4: Dezvoltarea tactică**
  Elementele acestui nivel sunt concepute pentru a dezvolta metode mai bune și mai proactive de detectare a atacurilor și de reacție la acestea. Până la acest nivel, majoritatea metodelor de prevenire ar trebui să fie puse în aplicare.
- **Nivelul 5: Capacitate operațională de securitate deplină**
  Acest nivel reprezintă elementele care ar trebui să fie instituite pentru ca orice organizație să se considere pe deplin pregătită din punct de vedere operațional să abordeze orice tip de amenințare cibernetică.

Figura 31: Rezumatul dimensiunilor CCSMM per nivel

	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	Nivelul 1
Security Aware	Sensibilizare cu privire la securitate
Level 2	Nivelul 2
Process Development	Dezvoltarea proceselor
Level 3	Nivelul 3
Information Enabled	Bazat pe informații
Level 4	Nivelul 4
Tactics Development	Dezvoltarea tactică
Level 5	Nivelul 5
Full Security Operational Capability	Capacitate operațională de securitate deplină
Threats Addressed	amenințări abordate
Metrics	indicatori
Information sharing	schimb de informații
Technology	tehnologie
Training	formare
Test	test
Unstructured	Nestructurat

Governement	Guvern
Industry	Industrie
Citizens	Cetățeni
Information Sharing Committee	Comitetul pentru schimbul de informații
Rosters, GETS, Assess Controls, Encryption	Rosters, GETS, controale de acces, criptare
1-dat Community Seminar	Seminar comunitar de 1 zi
Dark Screen – EOC	Dark Screen – EOC
Unstructured	Nestructurat
Governement	Guvern
Industry	Industrie
Citizens	Cetățeni
Community Security Web site	Site-ul web al securității comunitare
Secure Web Site Firewalls, Backups	Firewall-uri pentru un site de internet securizat, copii de rezervă
Conudcting a CCSE	Conducerea unui CCSE
Community Dark Screen	Dark Screen comunitar
Structured	Structurat
Governement	Guvern
Industry	Industrie
Citizens	Cetățeni
Information Correlation Center	Centrul de corelare a informațiilor
Event Correlation SW IDS/IPS	Corelarea evenimentelor SW IDS/IPS
Vulnerability Assessment	Evaluarea vulnerabilităților
Operational Dark Screen	Dark Screen operațional
Structured	Structurat
Governement	Guvern
Industry	Industrie
Citizens	Cetățeni
State/Fed Correlation	Corelare la nivel de stat/federal
24/7 manned operations	Operațiuni cu echipaj disponibile 24 de ore din 24, 7 zile din 7
Operational Security	Securitate operațională
Limited Black Demon	Black Demon limitat
Highly Structured	Înalt structurat
Governement	Guvern
Industry	Industrie
Citizens	Cetățeni
Complete Info Vision	Vedere integrală asupra informațiilor
Automated Operations	Operațiuni automatizate
Multi-Discipline Red Teaming	Red teaming multidisciplinar
Black Demon	Black Demon

Metodă de evaluare

CCSMM ca metodologie de evaluare este menită să fie implementată de comunități, cu contribuții din partea agențiilor de aplicare a legii de stat și federale. Scopul său este de a sprijini comunitatea să definească ceea ce este cel mai important, care sunt țintele cele mai probabile și ce anume trebuie protejat (și în ce măsură). Având în vedere aceste obiective, pot fi elaborate planuri pentru a aduce fiecare aspect al comunității la nivelul necesar de maturitate a securității cibernetice. Informațiile specifice generate de CCSMM contribuie la definirea obiectivelor diferitelor teste și exerciții care pot fi utilizate pentru a măsura eficacitatea programelor stabilite.

A.7 Modelul de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST (ISMM)

Modelul de maturitate a securității informațiilor (ISMM) a fost dezvoltat în cadrul Colegiului de Informatică și Inginerie al Universității de Petrol și Minerale Regele Fahd din Arabia Saudită. Acesta propune un nou model de maturitate a capacităților pentru a evalua punerea în aplicare a măsurilor de securitate cibernetică. Obiectivul ISMM este de a permite organizațiilor să evalueze progresele înregistrate în punerea în aplicare de-a lungul timpului, utilizând în mod regulat același instrument de măsurare pentru a se asigura că poziția de securitate dorită este menținută. ISMM a fost elaborat în 2017.

Atribute/Dimensiuni

ISMM se bazează pe domeniile evaluate existente ale cadrului NIST și adaugă o dimensiune privind evaluarea conformității. Aceasta face ca modelul să ajungă la **23 de domenii evaluate** pentru poziția de securitate a unei organizații. Cele 23 de domenii evaluate sunt:

i gestionarea activelor;
ii mediul de afaceri;
iii guvernanță;
iv evaluarea riscului;
v strategia de gestionare a riscurilor;
vi evaluarea conformității;
vii controlul accesului;
viii sensibilizare și formare;
ix securitatea datelor;
x procesele și procedurile de protecție a informațiilor;
xi întreținere;
xii tehnologie de protecție;
xiii anomalii și evenimente;
xiv monitorizarea continuă a securității;
xv procesele de detectare;
xvi planificarea răspunsului;
xvii comunicații de răspuns;
xviii analiza răspunsului;
xix atenuarea răspunsului;
xx îmbunătățiri ale răspunsului;
xxi planificarea redresării;
xxii îmbunătățiri ale redresării și
xxiii comunicații de recuperare.

Niveluri de maturitate

ISMM se bazează pe **5 niveluri de maturitate**, care, din păcate, nu sunt detaliate în documentația disponibilă.

- **Nivelul 1:** Proces realizat;
- **Nivelul 2:** Proces gestionat;
- **Nivelul 3:** Proces stabilit;
- **Nivelul 4:** Proces previzibil și
- **Nivelul 5:** Proces de optimizare.

Metodă de evaluare

ISMM nu propune nicio metodologie specifică pentru efectuarea evaluării pentru organizații.

A.8 Modelul de măsurare a capacității auditului intern (IA-CM) pentru sectorul public

Modelul de măsurare a capacității auditului intern (IA-CM) a fost elaborat de Fundația de Cercetare a Institutului Auditorilor Interni cu intenția de a consolida capacitățile și activitățile de sensibilizare prin autoevaluare în sectorul public. Destinat profesioniștilor din domeniul auditului, IA-CM oferă o imagine de ansamblu asupra modelului în sine, împreună cu un ghid de aplicare pentru a ajuta la utilizarea modelului ca instrument de autoevaluare.

Deși IA-CM se axează mai degrabă pe capacitatea de audit intern decât pe consolidarea capacităților de securitate cibernetică, modelul este conceput ca un instrument de autoevaluare a maturității pentru entitățile din sectorul public, care poate fi aplicat la nivel mondial pentru a îmbunătăți procesele și eficacitatea. Întrucât domeniul de aplicare nu este axat pe securitatea cibernetică, nu vor fi analizate atributele. IA-CM a fost finalizat în 2009.

Niveluri de maturitate

Modelul de măsurare a capacității auditului intern (IA-CM) include **5 niveluri de maturitate**, fiecare dintre acestea descriind caracteristicile și capacitățile unei activități de audit intern la nivelul respectiv. Nivelurile de capacități din cadrul modelului oferă o foaie de parcurs pentru îmbunătățire continuă.

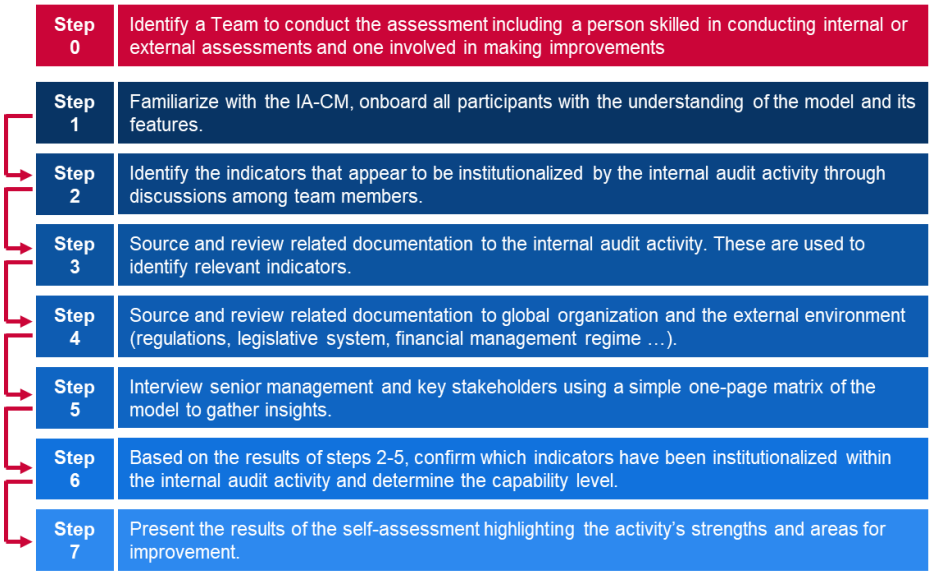
- **Nivelul 1: Inițial**
  Nu există capacități durabile, repetabile – dependente de eforturile individuale
  - ad-hoc sau nestructurat.
  - audituri sau analize unice izolate ale documentelor și tranzacțiilor pentru a verifica exactitatea și conformitatea.
  - rezultate în funcție de competențele persoanei care deține postul în cauză.
  - nu există alte practici profesionale decât cele furnizate de asociațiile profesionale.
  - aprobarea finanțării de către conducere, după caz.
  - lipsa infrastructurii.
  - auditorii pot face parte dintr-o unitate organizațională mai mare.
  - capacitatea instituțională nu este dezvoltată.
- **Nivelul 2: Infrastructură**
  practici și proceduri durabile și repetabile
  - întrebarea sau provocarea cheie pentru nivelul 2 este modul de stabilire și menținere a repetabilității proceselor și, prin urmare, a unei capacități repetabile.
  - relațiile de raportare a auditurilor interne, infrastructurile administrative și de gestionare, precum și practicile și procesele profesionale sunt în curs de stabilire (orientări, procese și proceduri de audit intern).
  - planificarea auditului se bazează în principal pe prioritățile de gestionare.
  - încrederea continuă, în esență, în aptitudinile și competențele anumitor persoane.
  - conformitate parțială cu standardele.
- **Nivelul 3: Integrat**
  practici profesionale și de gestionare aplicate în mod uniform
  - politicile, procesele și procedurile de audit intern sunt definite, documentate și integrate între ele și în infrastructura organizației.
  - gestionarea auditului intern și practicile profesionale sunt bine stabilite și aplicate în mod uniform în cadrul activității de audit intern.
  - auditul intern începe să se alinieze la activitatea organizației și la riscurile cu care aceasta se confruntă.
  - auditul intern evoluează de la efectuarea doar a unui audit intern tradițional la integrarea în echipă și furnizarea de consiliere cu privire la performanța și gestionarea riscurilor.
  - accentul se pune pe consolidarea echipei și pe capacitatea activității de audit intern, precum și pe independența și obiectivitatea acesteia.
  - în general, respectă standardele.
- **Nivelul 4: Gestionat**
  integrează informații din întreaga organizație pentru a îmbunătăți guvernanța și gestionarea riscurilor
  - auditul intern și așteptările principalelor părți interesate sunt în concordanță.
  - există indicatori de performanță pentru măsurarea și monitorizarea proceselor și rezultatelor auditului intern.
  - se recunoaște că auditul intern aduce contribuții semnificative organizației.
  - funcțiile de audit intern fac parte integrantă din guvernanța și gestionarea riscurilor organizației.
  - auditul intern este o unitate operațională bine gestionată.
  - riscurile sunt evaluate și gestionate cantitativ.
  - există aptitudinile și competențele necesare cu o capacitate de reînnoire și de partajare a cunoștințelor (în cadrul auditului intern și în cadrul organizației).
- **Nivelul 5: Optimizare**
  învățare din interiorul și din afara organizației în vederea îmbunătățirii continue
  - auditul intern este o organizație de învățare cu îmbunătățiri continue ale procesului și cu inovare.
  - auditul intern utilizează informații din interiorul și din afara organizației pentru a contribui la atingerea obiectivelor strategice.
  - performanță de nivel mondial/recomandată/cea mai bună practică.

- auditul intern este o parte esențială a structurii de guvernanță a organizației.
- competențe profesionale și specializate de nivel înalt.
- măsurile privind performanța individuală, unitară și organizațională sunt pe deplin integrate pentru
- stimularea îmbunătățirii performanțelor.

Metodă de evaluare

Modelul de măsurare a capacității auditului intern este conceput în mod clar pentru autoevaluare. Acesta prevede etapele detaliate care trebuie parcurse pentru utilizarea IA-CM și un pachet de eșantioane de slide-uri pentru personalizare. Înainte de începerea autoevaluării, trebuie identificată o echipă specifică, inclusiv cel puțin o persoană calificată să efectueze evaluări interne sau externe ale auditurilor interne și o persoană care este implicată în realizarea de îmbunătățiri în acest domeniu.

Figura 12: Etapele de autoevaluare ale IC-AM



Step 0	Etapa 0
Step 1	Etapa 1
Step 2	Etapa 2
Step 3	Etapa 3
Step 4	Etapa 4
Step 5	Etapa 5
Step 6	Etapa 6
Step 7	Etapa 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Identificarea unei echipe care să efectueze evaluarea, inclusiv a unei persoane calificate să efectueze evaluări interne sau externe și a unei persoane implicate în realizarea de îmbunătățiri.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Familiarizarea cu IA-CM, oferind tuturor participanților înțelegerea modelului și a caracteristicilor acestuia.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identificarea indicatorilor care par a fi instituționalizați de activitatea de audit intern prin discuții între membrii echipei.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Documentația privind sursa și analiza aferentă activității de audit intern. Aceștia sunt utilizați pentru a identifica indicatorii relevanți.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Documentația privind sursa și analiza aferentă organizației globale și mediului extern (regulamente, sistem legislativ, regim de gestiune financiară etc.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Realizarea de interviuri cu personalul de conducere de nivel superior și principalele părți interesate utilizând o matrice simplă de o pagină a modelului pentru a colecta informații.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Pe baza rezultatelor etapelor 2-5, confirmarea indicatorilor care au fost instituționalizați în cadrul activității de audit intern și determinarea nivelului capacității.

Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Prezentarea rezultatelor autoevaluării, evidențiind punctele forte ale activității și domeniile în care sunt necesare îmbunătățiri.

A.9 Indicele global de securitate cibernetică (GCI)

Indicele global de securitate cibernetică (GCI) este o inițiativă a Uniunii Internaționale a Telecomunicațiilor (UIT) care vizează revizuirea angajamentului și a situației în materie de securitate cibernetică în toate regiunile UIT: Africa, America, statele arabe, Asia-Pacific, CSI și Europa și care pune în centrul atenției țările cu un nivel ridicat de angajament și practici recomandate. Obiectivul GCI este de a sprijini țările să identifice domeniile în care se pot aduce îmbunătățiri în domeniul securității cibernetice, precum și de a le motiva să ia măsuri pentru a-și îmbunătăți poziția, contribuind astfel la creșterea nivelului general de securitate cibernetică la nivel mondial.

Întrucât GCI este un indice și nu un model de maturitate, acesta nu utilizează niveluri de maturitate, ci mai degrabă un punctaj pentru a clasifica și a compara angajamentul global în materie de securitate cibernetică al națiunilor și regiunilor.

Atribute/Dimensiuni

Indicele global de securitate cibernetică (GCI) se bazează pe cei cinci piloni ai Agendei globale privind securitatea cibernetică (GCA). Acești piloni formează cei cinci subindici ai GCI și fiecare include un set de indicatori. Cei cinci piloni și indicatori sunt după cum urmează:

i **Juridic**: măsuri bazate pe existența instituțiilor și a cadrelor juridice care se ocupă de securitatea cibernetică și criminalitatea informatică.
- legislația privind criminalitatea informatică;
- reglementarea securității cibernetice și
- limitarea legislației privind spamul.

ii **Tehnică**: măsuri bazate pe existența instituțiilor și a cadrelor tehnice care vizează securitatea cibernetică.
- CERT/CIRT/CSRIT;
- cadrul de implementare a standardelor;
- organismul de standardizare;
- mecanismele și capacitățile tehnice aplicate pentru a aborda problema Spam-ului;
- utilizarea cloud-ului în scopuri de securitate cibernetică și
- mecanisme de protecție online a copiilor.

iii **Organizațională**: măsuri bazate pe existența unor instituții și strategii de coordonare a politicilor pentru dezvoltarea securității cibernetice la nivel național.
- strategia națională de securitate cibernetică;
- agenția responsabilă și
- securitate cibernetică.

iv **Consolidarea capacităților**: măsuri bazate pe existența unor programe de cercetare și dezvoltare, de educație și formare, a unor profesioniști autorizați și a unor agenții din sectorul public care promovează consolidarea capacităților.
- campanii de sensibilizare;
- cadrul pentru certificarea și acreditarea profesioniștilor din domeniul securității cibernetice;
- cursuri de formare profesională în domeniul securității cibernetice;
- programe educaționale sau programa academică în domeniul securității cibernetice;
- programe C&D în materie de securitate cibernetică și
- mecanisme de stimulare.

v **Cooperare**: măsuri bazate pe existența parteneriatelor, a cadrelor de cooperare și a rețelelor de schimb de informații.
- acorduri bilaterale;
- acorduri multilaterale;
- participarea la foruri/asociații internaționale;
- parteneriate public-privat;
- parteneriate inter-agenții/intra-agenție;

- cele mai bune practici.

Metodă de evaluare

GCI este un instrument de autoevaluare creat prin intermediul unui sondaj[30] cu întrebări binare, precodificate și deschise. Utilizarea răspunsurilor binare elimină evaluarea bazată pe opinie și orice posibilă parțialitate față de anumite tipuri de răspunsuri. Răspunsurile precodificate economisesc timp și permit o analiză mai precisă a datelor. În plus, o scară dihotomă simplă permite o evaluare mai rapidă și mai complexă deoarece nu necesită răspunsuri lungi, ceea ce accelerează și simplifică procesul de furnizare a răspunsurilor și de evaluare ulterioară. Respondentul ar trebui doar să confirme prezența sau lipsa anumitor soluții de securitate cibernetică identificate în prealabil. Un mecanism de sondaj online, care este utilizat pentru colectarea răspunsurilor și încărcarea materialelor relevante, permite extragerea de bune practici și un set de evaluări calitative tematice efectuate de un grup de experți.

Procesul global GCI este pus în aplicare după cum urmează:

- tuturor participanților li se trimite o scrisoare de invitație, prin care aceștia sunt informați cu privire la inițiativă și li se solicită un punct de contact responsabil cu colectarea tuturor datelor relevante și cu completarea chestionarului GCI online. În timpul sondajului online, punctul de contact aprobat este invitat oficial de UIT să răspundă la chestionar;
- Colectarea datelor primare (pentru țările care nu răspund la chestionar):
  - UIT elaborează un proiect inițial de răspuns la chestionar, utilizând date accesibile publicului și cercetare online;
  - proiectul de chestionar este trimis punctelor de contact pentru revizuire;
  - punctele de contact îmbunătățesc acuratețea și apoi returnează proiectul de chestionar;
  - proiectul de chestionar corectat este trimis fiecărui punct de contact în vederea aprobării finale și
  - chestionarul validat este utilizat pentru analiză, punctare și clasificare.
- Colectarea de date secundare (pentru țările care răspund la chestionar):
  - UIT identifică răspunsurile lipsă, documentele justificative, linkurile etc.;
  - punctul de contact îmbunătățește acuratețea reacțiilor, dacă este necesar;
  - proiectul de chestionar corectat este trimis fiecărui punct de contact în vederea aprobării finale și
  - chestionarul validat este utilizat pentru analiză, punctare și clasificare.

A.10 Indicele de putere cibernetică (CPI)

Indicele de putere cibernetică (CPI) a fost creat prin programul de cercetare al Unității de informații a grupului Economist (Economist Intelligence Unit), sponsorizat de Booz Allen Hamilton în 2011. CPI este un „model cantitativ și calitativ dinamic, [...] care măsoară atributele specifice ale mediului cibernetic în cadrul a patru factori determinanți ai puterii cibernetice: cadrul juridic și de reglementare; contextul economic și social; infrastructura tehnologică și aplicațiile industriale, care examinează progresele înregistrate în domeniul digital în sectoarele industriale cheie”[31]. Obiectivul indicelui de putere cibernetică este să efectueze analiza comparativă a capacității țărilor G20 de a rezista atacurilor cibernetice și să implementeze infrastructura digitală necesară pentru o economie prosperă și sigură. Criteriul de referință furnizat de CPI se concentrează asupra a 19 țări din G20 (excluzând UE). Indicele oferă în consecință un clasament al țărilor pentru fiecare indicator.

Atribute/Dimensiuni

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf
[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

Indicele de putere cibernetică (CPI) se bazează pe patru factori determinanți ai puterii cibernetice. Fiecare categorie este evaluată prin intermediul unei serii de indicatori, pentru a oferi fiecărei țări un punctaj specific. Categoriile și pilonii sunt după cum urmează:

i **Cadrul juridic și de reglementare**
- angajamentul guvernului față de dezvoltarea cibernetică
- politici de protecție cibernetică
- cenzura cibernetică (sau lipsa acesteia)
- eficacitate politică
- protecția proprietății intelectuale

ii **Contextul economic și social**
- niveluri de educație
- aptitudini tehnice
- deschiderea schimburilor comerciale
- gradul de inovare în mediul de afaceri

iii **Infrastructura tehnologică**
- accesul la tehnologia informației și comunicațiilor
- calitatea tehnologiei informației și comunicațiilor
- accesibilitatea din punct de vedere financiar a tehnologiei informației și comunicațiilor
- cheltuieli legate de tehnologia informației
- numărul de servere securizate

iv **Aplicație în industrie**
- rețele inteligente
- e-sănătate
- comerț electronic
- transport inteligent
- guvernare electronică

Metodă de evaluare

CPI este un model de evaluare cantitativă și calitativă. Evaluarea a fost efectuată de Unitatea de informații a grupului Economist (Economist Intelligence Unit) utilizând indicatori cantitativi din surse statistice disponibile și realizând estimări atunci când datele lipseau. Principalele surse utilizate sunt Unitatea de informații a grupului Economist (Economist Intelligence Unit); Organizația Națiunilor Unite pentru Educație, Știință și Cultură (UNESCO); Uniunea Internațională a Telecomunicațiilor (UIT);

A.11 Indicele de putere cibernetică (CPI)

Prezenta secțiune sintetizează principalele constatări ale analizei modelelor de maturitate existente. Tabelul 5: Prezentare generală a modelelor **de maturitate** oferă o imagine de ansamblu asupra principalelor caracteristici ale fiecărui model în conformitate cu modelul Becker modificat. Tabelul 6 Comparație între nivelurile de maturitate definițiile de nivel înalt ale nivelurilor de maturitate ale modelelor analizate. Tabelul 7 oferă o imagine de ansamblu asupra dimensiunilor sau atributelor utilizate în fiecare model.

Tabelul 5: Prezentare generală a modelelor de maturitate

Denumirea modelului	Instituția-sursă	Scop	Obiectiv	Numărul de niveluri	Numărul de atribute	Metoda de evaluare	Reprezentarea rezultatelor
Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM)	Global Cybersecurity Capacity Centre Universitatea Oxford	Să crească dimensiunea și eficacitatea consolidării capacităților în materie de securitate cibernetică la nivel internațional	Țări	5	5 dimensiuni principale	Colaborarea cu organizațiile locale în vederea perfecționării modelului înainte de a-l aplica la contextul național	Radar cu cinci secțiuni
Modelul de maturitate a capacității de securitate cibernetică (C2M2)	Departamentul pentru Energie al SUA (DOE)	Să sprijine organizațiile să își evalueze programele de securitate cibernetică și să aducă îmbunătățiri acestora și să își consolideze reziliența operațională	Organizații din toate sectoarele, de toate tipurile și dimensiunile	4	10 domenii principale	Metodologie și set de instrumente pentru autoevaluare	Card de punctaj cu diagrame inelare
Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice	Institutul național pentru standarde și tehnologie (National Institute of Standards and Technology – NIST)	Cadru care vizează orientarea activităților de securitate cibernetică și gestionarea riscurilor în cadrul organizațiilor	Organizații	N/A (4 niveluri)	5 funcții de bază	Autoevaluare	-
Modelul de maturitate a capacității de securitate cibernetică al Qatarului (Q-C2M2)	Colegiul de Drept al Universității Qatar	Furnizarea unui model funcțional care să poată fi utilizat pentru a evalua, a măsura și a dezvolta cadrul de securitate cibernetică al Qatarului	Organizații din Qatar	5	5 domenii principale	-	-
Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)	Departamentul Apărării din SUA (DOD)	Promovarea celor mai bune practici în materie de securitate cibernetică pentru protejarea informațiilor	Organizații din sectorul bazei industriale de apărare (DIB)	5	17 domenii principale	Evaluarea de către auditori terți	-
Modelul comunitar de maturitate în materie de securitate cibernetică (CCSMM)	Centrul pentru Asigurarea Infrastructurii și Securității al Universității din Texas	Stabilirea statutului actual al unei comunități în ceea ce privește pregătirea sa în domeniul cibernetic și furnizarea unei foi de parcurs pe care comunitățile să o urmeze în eforturile lor de pregătire	Comunități (administrații locale sau ale statelor)	5	6 dimensiuni principale	Evaluare în cadrul comunităților, cu contribuții din partea agenților de aplicare a legii de stat și federale	-
Model de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST (ISMM)	Colegiul de Informatică și Inginerie al Universității de Petrol și Minerale Regele Fahd, Dhahran, Arabia Saudită	Să permită organizațiilor să măsoare progresele înregistrate în punerea lor în aplicare de-a lungul timpului pentru a se asigura că își mențin poziția de securitate dorită	Organizații	5	23 de domenii evaluate	-	-
Modelul de măsurare a capacității auditului intern (IA-CM) pentru sectorul public	Fundația de Cercetare a Institutului Auditorilor Interni (The Institute of Internal auditors Research Foundation)	Să consolideze capacitatea de audit intern și activitățile de sensibilizare prin autoevaluare în sectorul public	Organizații din sectorul public	5	6 elemente	Autoevaluare	-

Indicele global de securitate cibernetică (GCI)	Uniunea Internațională a Telecomunicațiilor (UIT)	Să revizuiască angajamentul și situația în materie de securitate cibernetică și să sprijine țările să identifice domeniile în care se pot aduce îmbunătățiri în domeniul securității cibernetice;	Țări	N/A	5 piloni	Autoevaluarea	Tabel de clasificare
Indicele de putere cibernetică (CPI)	The Economist Intelligence Unit & Booz Allen Hamilton	Să efectueze analiza comparativă a capacității țărilor G20 de a rezista atacurilor cibernetice și să implementeze infrastructura digitală necesară pentru o economie prosperă și sigură.	Țările G20	N/A	4 categorii	Analiza comparativă realizată de Unitatea de informații a grupului Economist (Economist Intelligence Unit)	Tabel de clasificare

Tabelul 6 Comparație între nivelurile de maturitate

Model	Nivelul 1	Nivelul 2	Nivelul 3	Nivelul 4	Nivelul 5
Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM)	**Inițial** Fie nu există maturitate în materie de securitate cibernetică, fie aceasta este embrionară. Ar putea exista discuții inițiale cu privire la consolidarea capacităților în materie de securitate cibernetică, dar nu au fost luate măsuri concrete. În această etapă nu există dovezi observabile.	**Formativ** unele caracteristici ale aspectelor au început să se dezvolte și să fie formulate, dar pot fi ad-hoc, dezorganizate, slab definite sau pur și simplu „noi”. Cu toate acestea, dovada acestei activități poate fi demonstrată în mod clar.	**Stabilit** elementele acestui aspect există și funcționează. Cu toate acestea, nu există o analiză bine gândită a alocării relative a resurselor. S-au luat puține decizii bazate pe compromis în ceea ce privește investițiile „relative” în diferitele elemente ale acestui aspect. Cu toate acestea, aspectul este funcțional și definit.	**Strategic** s-au făcut alegeri cu privire la părțile aspectului care sunt importante și care sunt mai puțin importante pentru organizația sau națiunea respectivă. Etapa strategică reflectă faptul că aceste alegeri au fost efectuate în funcție de situația națiunii sau a organizației.	**Dinamic** Există mecanisme clare de modificare a strategiei în funcție de circumstanțele predominante, cum ar fi tehnologia mediului de amenințări, conflictul global sau o schimbare semnificativă într-un domeniu de interes (de exemplu, criminalitatea informatică sau protejarea vieții private). Organizațiile dinamice au elaborat metode de modificare a strategiilor. Procesul decizional rapid, realocarea resurselor și atenția constantă acordată mediului în schimbare sunt caracteristice acestei etape.
Modelul de maturitate a capacității de securitate cibernetică (C2M2)	**MIL0** Practicile nu sunt aplicate.	**MIL1** Practicile inițiale sunt aplicate, dar pot fi ad-hoc.	**MIL2** Caracteristici de gestionare: practicile sunt documentate; sunt puse la dispoziție resurse adecvate pentru a sprijini procesul; personalul care aplică practicile are competențe și cunoștințe adecvate și se atribuie responsabilitatea și autoritatea pentru punerea în aplicare a practicilor. Caracteristici de abordare: practicile sunt mai complete sau mai avansate decât la MIL1.	**MIL3** Caracteristici de gestionare: activitățile sunt ghidate de politici (sau de alte directive organizaționale); obiectivele de performanță pentru activitățile din domeniu sunt stabilite și monitorizate pentru a urmări rezultatele obținute și practicile documentate pentru activitățile din domeniu sunt standardizate și îmbunătățite la nivelul întreprinderii. Caracteristici de abordare:	-

				practicile sunt mai complete sau mai avansate decât la MIL2.	
Modelul de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST (ISMM)	**Proces realizat;**	**Proces gestionat;**	**Proces stabilit;**	**Proces previzibil și**	**Proces de optimizare.**
Modelul de maturitate a capacității de securitate cibernetică al Qatarului (Q-C2M2)	**Inițiere** Se utilizează practici și procese ad-hoc în materie de securitate cibernetică în unele domenii.	**Dezvoltare** S-au pus în aplicare politici și practici pentru dezvoltarea și îmbunătățirea activităților legate de securitatea cibernetică din domeniile respective, cu scopul de a sugera noi activități care să fie puse în aplicare.	**Aplicare** S-au adoptat politici de punere în aplicare a tuturor activităților legate de securitatea cibernetică din domeniile respective, cu scopul de a finaliza punerea în aplicare la un anumit moment.	**Adaptabil** Se reexaminează și se revizuiesc activitățile legate de securitatea cibernetică și se adoptă practici bazate pe indicatori predictivi derivați din experiențele și măsurile anterioare.	**Agil** Se practică în continuare etapa adaptabilă, punând un accent sporit pe agilitate și viteză în punerea în aplicare a activităților în domenii.
Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)	**Procese: Realizate** Întrucât organizația poate să aplice aceste practici doar ad-hoc și se poate baza sau nu pe documentație, maturitatea procesului nu este evaluată pentru nivelul 1. **Practici: Igienă cibernetică de bază** Nivelul 1 se axează pe protecția FCI (informații contractuale federale) și constă numai în practici care corespund cerințelor de bază în materie de protecție.	**Procese: Documentate** Nivelul 2 impune ca o organizație să stabilească și să documenteze practici și politici care să ghideze punerea în aplicare a eforturilor sale de CMMC. Documentarea practicilor permite persoanelor să le efectueze în mod repetabil. Organizațiile își dezvoltă capacități mature prin documentarea proceselor lor și apoi le practică astfel cum au fost documentate. **Practici: Igienă cibernetică intermediară** Nivelul 2 servește drept evoluție de la nivelul 1 la nivelul 3 și constă într-un subset de cerințe de securitate specificate în NIST SP 800-171, precum și practici din alte standarde și referințe.	**Procese: Gestionate** Nivelul 3 impune ca o organizație să elaboreze, să mențină și să pună la dispoziție un plan care să demonstreze gestionarea activităților pentru punerea în aplicare a practicilor. Planul poate include informații privind misiunile, obiectivele, planurile de proiect, resursele, formarea necesară și implicarea părților interesate relevante. **Practici: O bună igienă cibernetică**. Nivelul 3 se axează pe protecția CUI și cuprinde toate cerințele de securitate specificate în NIST SP 800-171, precum și practici suplimentare față de alte standarde și referințe pentru atenuarea amenințărilor.	**Procese: Revizuite.** Nivelul 4 impune ca o organizație să analizeze și să evalueze practicile din punctul de vedere al eficacității. Pe lângă practicile de evaluare a eficacității, organizațiile de la acest nivel sunt în măsură să ia măsuri corective atunci când este necesar și să informeze în mod recurent conducerea de nivel superior cu privire la statut sau probleme. **Practici: Proactive** Nivelul 4 se axează pe protecția CUI (informații neclasificate controlate) și cuprinde un subset al cerințelor de securitate consolidate. Aceste practici sporesc capacitățile de detectare și de răspuns ale unei organizații pentru a aborda și a se adapta la tactica, tehnicile și procedurile în schimbare.	**Procese: Optimizare** Nivelul 5 necesită ca o organizație să standardizeze și să optimizeze punerea în aplicare a proceselor în întreaga organizație. **Practici: Avansate/Proactive** Nivelul 5 se axează pe protecția CUI (informații neclasificate controlate). Practicile suplimentare sporesc profunzimea și complexitatea capacităților de securitate cibernetică.
Modelul comunitar de maturitate în materie de securitate cibernetică (CCSMM)	**Sensibilizare cu privire la securitate** Principala temă a activităților la acest nivel este de a sensibiliza persoanele și organizațiile cu privire la amenințările, problemele	**Dezvoltarea proceselor** Nivelul conceput pentru a sprijini comunitățile să instituie și să îmbunătățească procesele de securitate necesare în scopul de a aborda în mod eficace	**Bazat pe informații** Conceput pentru a îmbunătăți mecanismele de schimb de informații în cadrul comunității în scopul de a permite comunității să coreleze efectiv informații aparent disparate.	**Dezvoltarea tactică** Elementele acestui nivel sunt concepute pentru a dezvolta metode mai bune și mai proactive de detectare a atacurilor și de reacție la acestea. Până la acest nivel, majoritatea metodelor de	**Capacitate operațională de securitate deplină** Acest nivel reprezintă elementele care ar trebui să fie instituite pentru ca orice organizație să se considere pe deplin pregătită din punct de vedere operațional să

	și aspectele legate de securitatea cibernetică.	aspectele legate de securitatea cibernetică.		prevenire ar trebui să fie puse în aplicare.	abordeze orice tip de amenințare cibernetică.
Modelul de măsurare a capacității auditului intern (IA-CM) pentru sectorul public	**Inițiale** Nu există capacități durabile, repetabile – dependente de eforturile individuale	**Infrastructură** Practici și proceduri durabile și repetabile	**Integrate** Practici profesionale și de gestionare aplicate în mod uniform	**Gestionate** Integrează informații din întreaga organizație pentru a îmbunătăți guvernanța și gestionarea riscurilor	**Optimizare** Învățare din interiorul și din afara organizației în vederea îmbunătățirii continue

Tabelul 7: Compararea atributelor/dimensiunilor

	Modelul de maturitate a capacității de securitate cibernetică pentru națiuni (CMM)	Modelul de maturitate a capacității de securitate cibernetică (C2M2)	Modelul de maturitate a capacității de securitate cibernetică al Qatarului (Q-C2M2)	Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)	Certificarea modelului de maturitate în materie de securitate cibernetică (CMMC)	Modelul de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST (ISMM)	Cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice	Indicele global de securitate cibernetică (GCI)	Indicele de putere cibernetică (CPI)
Niveluri	Cinci dimensiuni, împărțite în mai mulți factori, incluzând mai multe aspecte și multipli indicatori (Figura 4)	Zece domenii, inclusiv un obiectiv unic de gestionare și mai multe obiective de abordare (Figura 6)	Cinci domenii împărțite în subdomenii	Șaptesprezece domenii detaliate în procese și una sau mai multe capacități, care sunt detaliate în continuare în practici (Figura 9).	Șase dimensiuni principale	Douăzeci și trei de domenii evaluate	Cinci funcții, cu categorii și subcategorii cheie subiacente (Figura 8).	Cinci piloni care includ mai mulți indicatori	Patru categorii cu mai mulți indicatori
Atribute/ dimensiuni	i elaborarea unei politici și a unei strategii în materie de securitate cibernetică; ii încurajarea unei culturi responsabile în materie de securitate cibernetică în societate; iii dezvoltarea cunoștințelor în materie de securitate cibernetică; iv crearea unor cadre juridice și de reglementare eficace și v controlul riscurilor prin standarde, organizații și tehnologii.	i gestionarea riscurilor; ii active, modificări și gestionarea configurației; iii gestionarea identității și a accesului; iv gestionarea amenințărilor și a vulnerabilităților; v conștientizarea situației; vi reacția la incidente și evenimente; vii gestionarea lanțului de aprovizionare și a dependențelor externe; viii gestionarea forței de muncă; ix arhitectura securității cibernetice; x gestionarea programului de securitate cibernetică.	i înțelegere (guvernanța cibernetică, activele, riscurile și formarea); ii securitizare (securitatea datelor, securitatea tehnologică, securitatea controlului accesului, securitatea comunicațiilor și securitatea personalului); iii expunere (monitorizare, gestionarea incidentelor, detectare, analiză și expunere); iv răspuns (planificarea răspunsului, atenuarea și comunicarea răspunsului);	i controlul accesului; ii gestionarea activelor; iii audit și responsabilitate; iv sensibilizare și formare; v gestionarea configurației; vi identificare și autentificare; vii reacția la incidente; viii întreținere; ix protecția mass-media; x securitatea personalului; xi protecție fizică; xii redresare; xiii gestionarea riscurilor; xiv evaluarea securității; xv conștientizarea situației; xvi protecția sistemelor și a comunicațiilor;	i amenințări abordate; ii indicatori; iii schimb de informații; iv tehnologie; v formare; vi test.	i gestionarea activelor; ii mediul de afaceri; iii guvernanță; iv evaluarea riscului; v strategia de gestionare a riscurilor; vi evaluarea conformității; vii controlul accesului; viii sensibilizare și formare; ix securitatea datelor; x procesele și procedurile de protecție a informațiilor; xi întreținerea; xii tehnologie de protecție; xiii anomalii și evenimente; xiv monitorizarea continuă a securității; xv procesele de detectare; xvi planificarea răspunsului;	i identificare; ii protejare; iii detectare; iv răspuns; v recuperare;	i juridic; ii tehnic; iii organizațional; iv consolidarea capacităților; v cooperare.	i cadrul juridic și de reglementare; ii contextul economic și social; iii infrastructura tehnologică; iv aplicație în industrie.

			v	susținere (planificarea redresării, gestionarea continuității, îmbunătățire și dependențe externe).	xvii	integritatea sistemelor și a informațiilor.		xvii xviii xix xx xxi xxii xxiii	comunicații de răspuns; analiza răspunsului; atenuarea răspunsului; îmbunătățiri ale răspunsului; planificarea redresării; îmbunătățiri ale redresării; comunicații de recuperare.

ANEXA B – BIBLIOGRAFIE DE CERCETARE DOCUMENTARĂ

Almuhammadi, S. și Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework" (Model de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST), în Computer Science & Information Technology (CS & IT). A șasea conferință internațională privind serviciile și convergența tehnologiei informației, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. și Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework" (Model de maturitate a securității informațiilor pentru cadrul de securitate cibernetică NIST), în Computer Science & Information Technology (CS & IT). Document disponibil la adresa: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs (Evaluare, analiză și recomandări privind protecția infrastructurilor critice de informații). Document disponibil la adresa: 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 (Dezvoltarea modelelor de maturitate pentru gestionarea IT – un model de procedură și aplicarea acestuia). Document disponibil la adresa: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Guvernul Belgiei (2012) Strategia de securitate cibernetică. Document disponibil la adresa: 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

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide (Dezvoltarea capacității de securitate cibernetică: un ghid de punere în aplicare pentru validarea conceptului). RAND Corporation. Document disponibil la adresa: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) "Introduction to Return on Security Investment" (Introducerea în rentabilitatea investițiilor în securitate).

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) "Cybersecurity Capability Maturity Model (C2M2)" (Modelul de maturitate a capacității de securitate cibernetică) Versiunea 2.0. Document disponibil la adresa: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland (Strategii naționale de securitate cibernetică în comparație - provocări pentru Elveția). Document disponibil la adresa: 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

Consiliul de Miniștri (2019) Jurnalul Oficial al Portugaliei, seria 1 – nr. 108 – Rezoluția Consiliului de Miniștri nr. 92/2019. Document disponibil la adresa: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (Modelul de maturitate a capacității de securitate cibernetică pentru națiuni) (CMM). Universitatea Oxford.

CSIRT Maturity - Self-assessment Tool (Maturitatea CSIRT – instrument de autoevaluare) (dată indisponibilă). Document disponibil la adresa: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Proiectul CyberCrime@IPA al Consiliului Europei și al Uniunii Europene, Proiectul global privind criminalitatea informatică al Consiliului Europei și Grupul operativ al Uniunii Europene pentru combaterea criminalității cibernetice (2011) Unități specializate în criminalitatea informatică – studiu privind bunele practici. Document disponibil la adresa: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Sistemul de raportare și analiză a incidentelor de securitate cibernetică – instrument de analiză vizuală (dată indisponibilă). Document disponibil la adresa: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (Parteneriate public-privat) (PPP).

Darra, E. (dată indisponibilă) “Welcome to the NCSS Training Tool” (Introducere la instrumentul de instruire SNSC).

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting (Orientări tehnice privind raportarea incidentelor). Document disponibil la adresa: 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 (Orientări tehnice privind măsurile de securitate). Document disponibil la adresa: 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 (Orientări privind amenințările și activele). Document disponibil la adresa: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Strategia de securitate cibernetică a Sloveniei. Document disponibil la adresa: 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 (Protecția vieții private și a datelor din faza de concepere – de la politică la inginerie).* Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Comisia Europeană (2012) Regulamentul Parlamentului European și al Consiliului privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă. Document disponibil la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (2012) NCSS: Practical Guide on Development and Execution (SNSC: Ghid practic de dezvoltare și realizare). Heraklion: ENISA.

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace (SNSC: Stabilirea cursului pentru eforturile naționale de consolidare a securității în spațiul cibernetic). Heraklion: ENISA.

Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (2016) Ghid pentru IMM-uri cu privire la securitatea prelucrării datelor cu caracter personal.

Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (2016) Ghid de bune practici privind SNSC: conceperea și punerea în aplicare a strategiilor naționale de securitate cibernetică. Heraklion: ENISA.

Uniunea Europeană și Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (2017) Manual privind securitatea prelucrării datelor cu caracter personal. Document disponibil la adresa: http://dx.publications.europa.eu/10.2824/569768

Uniunea Europeană și Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (2014) *Inventarul ENISA CERT al echipelor și al activităților CERT din Europa*. Document disponibil la adresa: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Biroul executiv al președintelui (2015), Memorandum pentru șefii departamentelor și agențiilor executive. Document disponibil la adresa: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Cancelaria Federală a Republicii Austria (2013) Strategia de securitate cibernetică a Austriei. Document disponibil la adresa: 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

Ministerul Federal al Internelor (2011) Strategia de securitate cibernetică pentru Germania. Document disponibil la adresa: 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

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 [Directiva NIS și legislația națională (2015) Standardele în materie de securitate a informațiilor și de protejare a vieții private pentru IMM-uri: recomandări pentru îmbunătățirea adoptării standardelor în materie de securitatea informațiilor și de protejare a vieții private în întreprinderile mici și mijlocii]. Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Uniunea Europeană și Agenția Europeană pentru Securitatea Rețelelor Informatice și a Informațiilor (2015) Raportul din 2015 privind exercițiile naționale și internaționale de securitate cibernetică: sondaj, analiză și recomandări. Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Biroul prim-ministrului francez (2014) Strategia de securitate digitală națională a Franței. Document disponibil la adresa: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

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 (Standardele în materie de securitate a informațiilor și de protejare a vieții private pentru IMM-uri: recomandări pentru îmbunătățirea adoptării standardelor în materie de securitatea informațiilor și de protejare a vieții private în întreprinderile mici și mijlocii). Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) “Evaluating Business Process Maturity Models” (Evaluarea modelelor de maturitate a proceselor operaționale), Journal of the Association for Information Systems. Document disponibil la adresa: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Guvernul Bulgariei (2015) Strategia națională de securitate cibernetică - Bulgaria rezilientă cibernetic 2020.

Guvernul Croației (2015) Strategia națională de securitate cibernetică a Republicii Croația. Document disponibil la adresa: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Guvernul Greciei (2017) Strategia națională de securitate cibernetică. Document disponibil la adresa: 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

Guvernul Ungariei (2018) Strategia pentru securitatea rețelelor și a sistemelor informatice. Document disponibil la adresa: 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

Guvernul Irlandei (2019) Strategia națională de securitate cibernetică. Document disponibil la adresa: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Guvernul Spaniei (2019) Strategia națională de securitate cibernetică. Document disponibil la adresa: 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

Institutul Auditorilor Interni (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide [Model de măsurare a capacității auditului intern (IA-CM) pentru sectorul public: prezentare generală și ghid de aplicare]. Altamonte Springs, Fla: Fundația de Cercetare a Institutului Auditorilor Interni.

Uniunea Internațională a Telecomunicațiilor (UIT) (2018) The Global Cybersecurity Index (Indicele global de securitate cibernetică). Document disponibil la adresa: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Uniunea Internațională a Telecomunicațiilor (UIT) (2018) Guide to developing a national cybersecurity strategy (Ghid pentru dezvoltarea unei strategii naționale de securitate cibernetică). Document disponibil la adresa: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) “Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework” (Către un model de maturitate a capacității de securitate cibernetică al Qatarului cu un cadru legislativ), International Review of Law.

Guvernul Letoniei (2014) Strategia de securitate cibernetică a Letoniei. Document disponibil la adresa: 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 (Un cadru de evaluare pentru strategiile naționale de securitate cibernetică). Heraklion: ENISA. Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks (Metodologii pentru identificarea activelor și serviciilor infrastructurilor critice de informații: orientări pentru configurarea rețelelor de comunicații electronice de date).* Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministerul Competitivității și Economiei Digitale, Maritime și a Serviciilor (2016) Strategia de securitate cibernetică a Maltei. Document disponibil la adresa: 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

Ministerul afacerilor economice și comunicațiilor (2019) Strategia națională de securitate cibernetică – Republica Estonia. Document disponibil la adresa: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerul Apărării Naționale al Republicii Lituania (2018) Strategia națională de securitate cibernetică

Centrul Național de Securitate Cibernetică (2015) Strategia națională de securitate cibernetică a Republicii Cehe. Document disponibil la adresa: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Strategiile naționale de securitate cibernetică – hartă interactivă (fără dată). Document disponibil la adresa: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Instrumentul de evaluare a strategiilor naționale de securitate cibernetică (2018). Document disponibil la adresa: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Institutul național pentru standarde și tehnologie (National Institute of Standards and Technology) (2018) Framework for Improving Critical Infrastructure Cybersecurity (Cadru pentru îmbunătățirea securității cibernetice a infrastructurii critice), versiunea 1.1. Gaithersburg, MD: Institutul național pentru standarde și tehnologie (National Institute of Standards and Technology). Document disponibil la adresa: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model (Modelul de maturitate a proceselor comerciale). Document disponibil la adresa: https://www.omg.org/spec/BPMM/1.0/PDF

OCDE, Uniunea Europeană și Centrul Comun de Cercetare – Comisia Europeană (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide (Manual privind crearea indicatorilor compoziți: metodologie și ghid de utilizare). OCDE. Document disponibil la adresa: https://www.oecd.org/sdd/42495745.pdf.

Biroul Comisarului pentru comunicații electronice și reglementări poștale (2012) Strategia de securitate cibernetică a Republicii Cipru.

Jurnalul Oficial al Uniunii Europene (2008) DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. Document disponibil la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Organizația pentru Cooperare și Dezvoltare Economică (OCDE) (2012) Cybersecurity policy making at a turning point (Elaborarea de politici de securitate cibernetică, într-un moment de cotitură). Document disponibil la adresa: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) “National Cyber Security Strategies - Practical Guide on Development and Execution” (Strategii naționale de securitate cibernetică – Ghid practic de dezvoltare și realizare).

Ouzounis, E. (2012) Good Practice Guide on National Exercises (Ghid de bune practici privind exercițiile naționale).

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects (Îmbunătățirea cooperării dintre CSIRT și autoritățile de aplicare a legii: aspecte juridice și organizaționale)

Președinția Consiliului de Miniștri (2017) Planul de acțiune privind securitatea cibernetică al Italiei. Document disponibil la adresa: 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

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

Guvernul României (2013) Strategia de securitate cibernetică a României. Document disponibil la adresa: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. și Agenția Uniunii Europene pentru Securitate Cibernetică (2019) Bunele practici în materie de inovare în domeniul securității cibernetice în cadrul SNSC: bunele practici în materie de inovare în domeniul securității cibernetice în cadrul strategiilor naționale

de securitate cibernetică. Document disponibil la adresa: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariatul Comitetului de Securitate (2019) Strategia de securitate cibernetică a Finlandei 2019. Document disponibil la adresa: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Guvernul slovac (2015) Conceptul de securitate cibernetică al Republicii Slovace. Document disponibil la adresa: 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

Smith, R. (2015) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016

Smith, R. (2016) „Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016", în Smith, R., Core EU Legislation (Legislația de bază a UE). Londra: Macmillan Education. Document disponibil la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017) European Cyber Security Month 2017 (Luna europeană a securității cibernetice în 2017).

Guvernul Suediei (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Document disponibil la adresa: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Guvernul Danemarcei - Ministerul de Finanțe (2018) Strategia de securitate cibernetică și a informațiilor a Danemarcei. Document disponibil la adresa: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Consiliul Federal (2018) Strategia națională pentru protecția Elveției împotriva riscurilor cibernetice.

Consiliul Guvernului din Luxemburg (2018) Strategia națională de securitate cibernetică. Document disponibil la adresa: 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

Guvernul Țărilor de Jos (2018) Agenda națională de securitate cibernetică. Document disponibil la adresa: 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

Casa Albă (2018) National Cyber Strategy of the United States of America (Strategia națională de securitate cibernetică a Statelor Unite ale Americii). Document disponibil la adresa: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report (Raportul privind Europa cibernetică). Document disponibil la adresa: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (2013) *National-level risk assessments: an analysis report (Evaluările riscurilor la nivel național: un raport de analiză).* Document disponibil la adresa: 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 (Raportul privind cooperarea și gestionarea crizelor cibernetice). Document disponibil la adresa: 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 (Raportul privind cooperarea și gestionarea crizelor cibernetice: practici comune de gestionare a crizelor

la nivelul UE și aplicabilitatea în cazul crizelor cibernetice). Document disponibil la adresa: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Regatul Unit – Strategia națională de securitate cibernetică pentru perioada 2016-2021 (2016). Document disponibil la adresa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Universitatea Innsbruck et al. (2009) Understanding Maturity Models (Înțelegerea modelelor de maturitate).

Wamala, D. F. (2011) "ITU National Cybersecurity Strategy Guide" (Ghidul privind strategia națională de securitate cibernetică a UIT). Document disponibil la adresa: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) "The Community Cyber Security Maturity Model" (Modelul comunitar de maturitate în materie de securitate cibernetică), în cadrul celei de-a 40-a Conferințe internaționale anuale din Hawaii privind științele sistemelor din 2007 (HICSS'07)

ANEXA C – ALTE OBIECTIVE STUDIATE

Obiectivele detaliate mai jos au fost studiate în cadrul etapei de cercetare documentară și al interviurilor realizate de ENISA. Următoarele obiective nu fac parte din cadrul de evaluare a capacităților naționale, dar pun în lumină subiecte care merită discutate. Fiecare dintre următoarele subcapitole va oferi o explicație cu privire la motivul pentru care obiectivul a fost eliminat.

- elaborarea unor strategii sectoriale în materie de securitate cibernetică;
- combaterea campaniilor de dezinformare;
- asigurarea de tehnologii de vârf (5G, IA, informatica cuantică etc.);
- asigurarea suveranității datelor și
- oferirea de stimulente pentru dezvoltarea sectorului asigurărilor cibernetice.

Elaborarea unor strategii sectoriale în materie de securitate cibernetică

Adoptarea unor strategii sectoriale specifice care vizează intervențiile și stimulentele sectoriale introduce cu siguranță o capacitate descentralizată mai puternică. Acest lucru este deosebit de potrivit pentru statele membre ale căror OSE trebuie să respecte cadre și reglementări diferite și unde există multe dependențe din cauza naturii transversale a securității cibernetice. Într-adevăr, în mai multe state membre este un lucru obișnuit să existe zeci de autorități naționale și organisme de reglementare care cunosc particularitățile fiecărui sector și care dețin un mandat de punere în aplicare a unor reglementări specifice pentru fiecare sector.

Danemarca, de exemplu, a lansat șase strategii specifice care abordează eforturile în materie de securitate cibernetică și a informațiilor din cele mai critice sectoare pentru a dezvolta o capacitate descentralizată mai puternică în domeniul securității cibernetice și a informațiilor. Fiecare „unitate sectorială” va contribui, printre altele, la evaluarea amenințărilor la nivel sectorial, la monitorizare, exerciții de pregătire, instituirea de sisteme de securitate, schimbul de cunoștințe și instrucțiuni. Strategiile sectoriale vizează următoarele sectoare:

- energie;
- sănătate;
- transport;
- telecomunicații;
- financiar și
- maritim.

Alte state membre și-au exprimat interesul de a examina posibilitatea unor strategii sectoriale de securitate cibernetică care să reflecte toate cerințele de reglementare. Cu toate acestea, trebuie remarcat faptul că un astfel de obiectiv ar putea să nu corespundă tuturor statelor membre, în funcție de dimensiunea lor, de politicile naționale și de gradul de maturitate al acestora. Dificultatea mare de a se asigura că acest cadru poate ține seama de toate particularitățile a determinat ENISA să nu includă acest obiectiv în cadru.

Combaterea campaniilor de dezinformare

Statele membre integrează protecția principiilor fundamentale, cum ar fi drepturile omului, transparența și încrederea publică, în strategiile lor naționale de securitate cibernetică. Acest

lucru este foarte important, în special în ceea ce privește dezinformarea care este difuzată prin intermediul platformelor de știri tradiționale sau al platformelor de comunicare socială. În plus, securitatea cibernetică este în prezent una dintre cele mai mari provocări electorale. Într-adevăr, au fost observate activități precum difuzarea de informații false sau propagandă negativă în diferite țări în perioada premergătoare unor alegeri importante. Această amenințare are potențialul de a submina procesul democratic în UE. La nivel european, Comisia a prezentat un plan de acțiune[32] pentru intensificarea eforturilor de combatere a dezinformării în Europa: planul se axează pe 4 domenii-cheie (detectare, cooperare, colaborare cu platformele online și sensibilizare) și servește la consolidarea capacităților UE și la consolidarea cooperării dintre statele membre.

4 din cele 19 țări intervievate și-au exprimat intenția de a aborda problema dezinformării și a propagandei în cadrul SNSC.

De exemplu, SNSC din Franța[33] menționează că: „este responsabilitatea statului să informeze cetățenii cu privire la riscurile tehnicilor de manipulare și propagandă utilizate de actorii răuvoitori pe internet. De exemplu, după atacurile teroriste împotriva Franței din ianuarie 2015, guvernul a instituit o platformă de informare privind riscurile legate de radicalizarea islamică prin intermediul rețelelor de comunicații electronice: « Stop-djihadisme.gouv.fr ».” Această abordare ar putea fi extinsă pentru a răspunde altor fenomene de propagandă sau destabilizare.

Într-un alt exemplu, SNSC 2019-2024 din Polonia[34] menționează că: „împotriva activităților de manipulare, cum ar fi campaniile de dezinformare, sunt necesare acțiuni sistemice pentru a spori gradul de conștientizare al cetățenilor în contextul verificării autenticității informațiilor și al răspunsului la tentativele de denaturare a acestora.”

Cu toate acestea, în cursul interviurilor realizate de ENISA, mai multe state membre au afirmat că nu abordează problema în cadrul propriei SNSC ca o amenințare la adresa securității cibernetice, ci mai degrabă o abordează la un nivel societal mai larg, de exemplu prin inițiative de politică.

Tehnologii de vârf securizate (5G, IA, informatica cuantică etc.)

Pe măsură ce actualul peisaj al amenințărilor cibernetice continuă să se extindă, dezvoltarea de noi tehnologii va conduce cel mai probabil la o creștere a intensității și a numărului de atacuri cibernetice și la diversificarea metodelor, a mijloacelor și a țintelor utilizate de factorii de amenințare. Între timp, aceste noi soluții tehnologice sub forma tehnologiilor de vârf au potențialul de a deveni elementele constitutive ale pieței digitale europene. Pentru a proteja dependența digitală tot mai mare a statelor membre și apariția de noi tehnologii, ar trebui să se instituie stimulente și politici de sine stătătoare pentru a sprijini dezvoltarea și implementarea sigură și fiabilă a acestor tehnologii în UE.

În cursul etapei de cercetare documentară efectuate cu privire la SNSC ale statelor membre, următoarele tehnologii de vârf au fost prezentate ca fiind de interes pentru statele membre: 5G, IA, calcul cuantic, criptografie, calcul de vârf, vehicule conectate și autonome, volume mari de date și date inteligente, tehnologia blockchain, robotica și internetul obiectelor.

[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
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

În special, la începutul anului 2020 Comisia Europeană a publicat o comunicare prin care invită statele membre să ia măsuri pentru punerea în aplicare a setului de măsuri recomandate în concluziile setului de instrumente 5Gs[35]. Acest set de instrumente 5G vine în urma Recomandării (UE) 2019/534 privind securitatea cibernetică a rețelelor 5G, adoptată de Comisie în 2019, care a solicitat o abordare europeană unificată a securității rețelelor 5G[36].

În cursul interviurilor realizate de ENISA, s-a subliniat faptul că acest subiect este mai degrabă un subiect transversal care este abordat în întreaga SNSC decât un obiectiv specific în sine.

Asigurarea suveranității datelor

Pe de o parte, spațiul cibernetic poate fi considerat un spațiu comun global formidabil, ușor accesibil, care oferă un grad ridicat de conectivitate și care poate genera oportunități importante de creștere socioeconomică. Pe de altă parte, spațiul cibernetic se caracterizează, de asemenea, prin jurisdicție slabă, dificultatea de a atribui acțiuni, lipsa frontierelor și sisteme interconectate care pot fi poroase și ale căror date pot fi furate sau chiar accesate de guvernele străine. Pe lângă aceste două perspective, ecosistemul digital este marcat de concentrarea platformelor și a infrastructurii de servicii online în mâinile unui număr foarte mic de părți interesate. Toate aspectele menționate anterior determină statele membre să promoveze suveranitatea digitală. Realizarea suveranității digitale înseamnă că cetățenii și întreprinderile sunt în măsură să prospere pe deplin prin utilizarea serviciilor digitale și a produselor TIC care sunt demne de încredere, fără a se teme pentru datele cu caracter personal sau activele digitale, autonomia economică sau influența politică a unei persoane.

Suveranitatea datelor sau suveranitatea digitală sunt promovate de statele membre la nivel național și european. Deși statele membre nu par să abordeze problema în mod direct în cadrul SNSC ca obiectiv specific, acestea fie o abordează ca un principiu transversal, fie își prezintă intenția de a asigura suveranitatea digitală la nivel național în publicații ad-hoc prin axare pe tehnologii-cheie. De exemplu, în revizuirea strategică a apărării cibernetice efectuată de Franța în 2018 se afirmă următoarele: „controlul următoarelor tehnologii este de o importanță capitală pentru asigurarea suveranității digitale: criptarea comunicațiilor, detectarea atacurilor cibernetice, radioul mobil profesionist, cloud computingul și inteligența artificială”[37].

La nivel european, statele membre participă activ la definirea strategiei europene privind datele (COM/2020/66 final) și la crearea cadrului UE de certificare pentru produsele, serviciile și procesele digitale TIC instituit prin Regulamentul UE privind securitatea cibernetică (2019/881) pentru a asigura autonomia digitală strategică la nivel european.

Etapa de intervievare cu statele membre a arătat că subiectul suveranității digitale este adesea considerat o chestiune mai amplă decât una care se limitează la securitatea cibernetică. Prin urmare, statele membre nu acoperă acest subiect în cadrul propriilor SNSC, iar puținele state care fac acest lucru nu îl acoperă ca obiectiv specific în sine.

Oferirea de stimulente pentru dezvoltarea sectorului asigurărilor cibernetice

Situația actuală a sectorului asigurărilor cibernetice arată că piața mondială a crescut fără îndoială. Aceasta este însă abia la început, întrucât trebuie colectate în continuare date și încă trebuie stabilite multe precedente (de exemplu, acoperirea tacită, riscurile cibernetice sistemice etc.). În plus, pierderile estimate cumulate în urma atacurilor cibernetice din întreaga lume sunt cu mai multe ordine de mărime mai mari decât actuala capacitate de acoperire a sectorului

[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/RO/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

asigurărilor cibernetice (Documentul de lucru al FMI – Riscul cibernetic pentru sectorul financiar: Un cadru pentru evaluarea cantitativă WP/18/143). Cu toate acestea, dezvoltarea sectorului asigurărilor cibernetice poate aduce cu siguranță beneficii și poate pune bazele unor mecanisme virtuoase. Într-adevăr, mecanismele de asigurare cibernetică pot contribui la:

- sensibilizarea întreprinderilor cu privire la riscurile de securitate cibernetică;
- evaluarea cantitativă a expunerii la riscuri cibernetice;
- îmbunătățirea gestionării riscurilor în materie de securitate cibernetică;
- acordarea de sprijin organizațiilor care sunt victime ale atacurilor cibernetice și
- acoperirea daunelor (materiale sau nu) provocate de un atac cibernetic.

Anumite state membre au început să lucreze pe această temă. De exemplu:

- Estonia a adoptat o abordare de tip „să așteptăm și să vedem ce se întâmplă” în cadrul SNSC: „Pentru a atenua riscurile cibernetice în sectorul privat în general, vor fi analizate cererea și oferta de servicii de asigurare cibernetică în Estonia și, pe această bază, se va conveni asupra unor principii de cooperare pentru părțile afiliate, inclusiv schimbul de informații, pregătirea evaluării riscurilor etc. Astăzi, pe piața estoniană sunt puțini furnizori de servicii de asigurare cibernetică și este necesar să se identifice mai întâi cine oferă un anumit serviciu. Complexitatea protecției asiguratorii este adesea considerată un obstacol în calea dezvoltării pieței asigurărilor cibernetice.”
- Luxemburg sprijină în mod specific dezvoltarea sectorului asigurărilor cibernetice în cadrul SNSC: „Obiectivul 1: Crearea de noi produse și servicii. Pentru a cumula riscurile și a încuraja victimele incidentelor cibernetice digitale să solicite ajutor din partea experților pentru a gestiona incidentul și a restabili un sistem afectat de un act rău intenționat, companiile de asigurări vor fi încurajate să creeze produse specifice pentru domeniul asigurărilor cibernetice.”

Răspunsurile primite de la persoanele intervievate au fost destul de diverse pe această temă: unele state membre au afirmat că tema asigurărilor cibernetice a devenit recent un subiect de discuție, în timp ce altele au fost de acord că, deși subiectul este promițător, sectorul nu este încă suficient de matur. Cu toate acestea, un număr mare de persoane intervievate au declarat că subiectul nu este abordat ca parte a SNSC, fie pentru că a fost considerat ca fiind prea specific, fie pentru că nu se încadrează în domeniul de aplicare a SNSC.

TP-06-20-047-EN-N

Despre Agenția Uniunii Europene pentru Securitate Cibernetică

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică contribuie la politica cibernetică a UE, îmbunătățește fiabilitatea produselor, serviciilor și proceselor TIC prin sistemele de certificare a securității cibernetice, cooperează cu statele membre și cu organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Pentru mai multe informații, consultați 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: 978-92-9204-491-6
DOI: 10.2824/29660