EUROPEAN UNION AGENCY
FOR CYBERSECURITY

OKVIR ZA PROCJENU NACIONALNIH KAPACITETA

PROSINAC 2020.

O ENISA-I

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije osnovana s ciljem postizanja visoke zajedničke razine kibersigurnosti u cijeloj Europi. Agencija Europske unije za kibersigurnost osnovana je 2004. na temelju Akta o kibersigurnosti EU-a i odonda pridonosi kiberpolitici EU-a, poboljšava pouzdanost proizvoda, usluga i postupaka IKT-a s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi na kiberizazove koji je očekuju u budućnosti. Razmjenom znanja, izgradnjom kapaciteta i informiranjem Agencija zajedno sa svojim ključnim dionicima radi na jačanju povjerenja u povezano gospodarstvo kako bi se povećala otpornost infrastrukture Unije i u konačnici zaštitila sigurnost europskog društva i građana. Više informacija dostupno je na: www.enisa.europa.eu.

KONTAKT

Za kontaktiranje s autorima obratite se na team@enisa.europa.eu.
Za medijske upite o ovom dokumentu obratite se na press@enisa.europa.eu.

AUTORI

Anna Sarri, Pinelopi Kyranoudi – Agencija Europske unije za kibersigurnost (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

ZAHVALE

ENISA zahvaljuje i odaje priznanje svim stručnjacima koji su sudjelovali i pružili vrijedan doprinos ovom izvješću, osobito onima navedenima u nastavku abecednim redom:

Centar za kibersigurnost (Belgija)

CFCS – Center for Cybersikkerhed (Danska), Thomas Wulff

Europski centar za kiberkriminalitet – EC3, Adrian-Ionut Bobeica

Europski centar za kiberkriminalitet – EC3, Alzofra Martinez Alvaro

Malteška agencija za informacijsku tehnologiju (Malta), Katia Bonello i Martin Camilleri

Ministarstvo digitalne politike (Grčka), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali i Sotiris Vasilos

Ministarstvo gospodarskih poslova i komunikacija (Estonija), Anna-Liisa Pärnalaas

Ministarstvo pravosuđa i javne sigurnosti (Norveška), Robin Bakke

Nacionalna agencija za kibersigurnost i informacijsku sigurnost (Češka), Veronika Netolická

Nacionalno sigurnosno tijelo (Slovačka)

NCTV, Ministarstvo pravosuđa i sigurnosti (Nizozemska)

Odjel za nacionalnu sigurnost (Španjolska), Maria Mar Lopez Gil

Odjel za politiku kibersigurnosti, Odjel za okoliš, klimu i komunikacije (Irska), James Caffrey

Portugalski Nacionalni centar za kibersigurnost (Portugal), Aleksandre Leite i Pedro Matos

Savezno ministarstvo unutarnjih poslova (Njemačka), Sascha-Alexander Lettgen

Središnji državni ured za razvoj digitalnog društva (Hrvatska), Marin Ante Pivčević

Sveučilište u Oxfordu — Centar za globalne kapacitete za kibersigurnost, Carolin Weisser Harris

Talijanska vlada (Italija)

Uprava za informacijsku sigurnost (Republika Slovenija), Marjan Kavčič

ENISA zahvaljuje na vrijednom doprinosu ovoj studiji i svim stručnjacima koji su u njoj sudjelovali, ali žele ostati anonimni.

PRAVNA OBAVIJEST

Mora se uzeti u obzir da ova publikacija predstavlja stajališta i tumačenja ENISA-e, osim ako je drukčije navedeno. Ovu publikaciju ne bi trebalo tumačiti kao pravni postupak ENISA-e ili tijela ENISA-e, osim ako je donesena u skladu s Uredbom (EU) 2019/881.
Ova publikacija ne predstavlja nužno najnovija zbivanja te je ENISA može povremeno ažurirati.

Prema potrebi citiraju se izvori trećih strana. ENISA nije odgovorna za sadržaj vanjskih izvora, uključujući vanjska mrežna mjesta navedena u ovoj publikaciji.

Ova je publikacija namijenjena isključivo u informativne svrhe. Mora biti besplatno dostupna. Ni ENISA ni bilo koja osoba koja djeluje u njezino ime nisu odgovorne za moguću uporabu informacija sadržanih u ovoj publikaciji.

OBAVIJEST O AUTORSKOM PRAVU

ISBN 978-92-9204-480-0

DOI: 10.2824/19

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

1. SADRŽAJ

O ENISA-I 1

KONTAKT 1

AUTORI 1

ZAHVALE 1

PRAVNA OBAVIJEST 2

OBAVIJEST O AUTORSKOM PRAVU 2

1. SADRŽAJ 3

POJMOVNIK 5

SAŽETAK 7

1. UVOD 9

1.1 OPSEG I CILJEVI STUDIJE 9

1.2 METODOLOŠKI PRISTUP 9

1.3 CILJNA PUBLIKA 10

2. KONTEKST 11

2.1 PRETHODNI RAD NA ŽIVOTNOM CIKLUSU NACIONALNE STRATEGIJE ZA KIBERSIGURNOST 11

2.2 ZAJEDNIČKI CILJEVI UTVRĐENI U OKVIRU EUROPSKE NACIONALNE STRATEGIJE ZA KIBERSIGURNOST 12

2.3 KLJUČNI ZAKLJUČCI IZ POSTUPKA UTVRĐIVANJA REFERENTNIH VRIJEDNOSTI 16

2.4 IZAZOVI PRI PROCJENI NACIONALNE STRATEGIJE ZA KIBERSIGURNOST 18

2.5 KORISTI OD NACIONALNE PROCJENE KAPACITETA 19

3. METODOLOGIJA OKVIRA ZA PROCJENU NACIONALNIH KAPACITETA 21

3.1 OPĆA SVRHA 21

3.2 RAZINE ZRELOSTI 21

3.3 KLASTERI I SVEOBUHVATNA STRUKTURA OKVIRA ZA SAMOPROCJENU 22

3.4 MEHANIZAM OCJENJIVANJA 23

3.5 ZAHTJEVI ZA OKVIR ZA SAMOPROCJENU 26

4. POKAZATELJI OKVIRA ZA PROCJENU NACIONALNIH KAPACITETA 27

4.1 POKAZATELJI IZ OKVIRA 27

4.2 SMJERNICE ZA PRIMJENU OKVIRA 55

5. SLJEDEĆI KORACI 57

5.1 BUDUĆA POBOLJŠANJA 57

PRILOG A — PREGLED REZULTATA ANALIZE DOKUMENTACIJE 58

PRILOG B – BIBLIOGRAFIJA ANALIZE DOKUMENTACIJE 86

PRILOG C – OSTALI ANALIZIRANI CILJEVI 92

POJMOVNIK

POKRATA	DEFINICIJA
AI	Umjetna inteligencija
C2M2	Model zrelosti kapaciteta u području kibersigurnosti
CCRA	Sporazum o zajedničkim kriterijima za priznavanje
CCSMM	Model zrelosti kibersigurnosti zajednice
CII	Ključna informatička infrastruktura
CMM	Model zrelosti kapaciteta u području kibersigurnosti za države
CMMC	Certifikacija modela zrelosti kibersigurnosti
CPI	Indeks kibersposobnosti
CSIRT	Timovi za odgovor na računalne sigurnosne incidente
CVD	Koordinirano otkrivanje ranjivosti
DČ	Država članica
DPA	Akt o zaštiti podataka
DSM	Jedinstveno digitalno tržište
ECCG	Europska skupina za kibersigurnosnu certifikaciju
ECSM	Europski mjesec kibersigurnosti
ECSO	Europska organizacija za kibersigurnost
EFTA	Europsko udruženje slobodne trgovine
EQF	Europski kvalifikacijski okvir
EU	Europska unija
GCI	Globalni indeks kibersigurnosti
GDPR	Opća uredba o zaštiti podataka
GDS	Državna digitalna služba
IA-CM	Model sposobnosti unutarnje revizije za javni sektor
IKT	Informacijska i komunikacijska tehnologija
ISMM	Model zrelosti informacijske sigurnosti za okvir kibersigurnosti NIST-a
ITU	Međunarodna unija za telekomunikacije
JPP	Javno-privatna partnerstva
LEA	Agencija za izvršavanje zakonodavstva

MSP-ovi	Mala i srednja poduzeća
NCSS	Nacionalne strategije za kibersigurnost
NIS	Mrežna i informacijska sigurnost
NIST	Nacionalni institut za norme i tehnologiju
NLO	Nacionalni časnici za vezu
OES	Operatori ključnih usluga
OT	Operativna tehnologija
PET	Tehnologije za unapređenje zaštite privatnosti
PIMS	Sustav upravljanja privatnošću informacija
Q-C2M2	Katarski model zrelosti kapaciteta u području kibersigurnosti
R&D	Istraživanje i razvoj
SOG-IS MRA	Skupina viših dužnosnika za sigurnost informacijskih sustava, Sporazum o uzajamnom priznavanju

SAŽETAK

Budući da su trenutačno kiberprijetnje i dalje u porastu, a intenzitet i broj kibernapada povećava, države članice EU-a trebaju djelotvorno reagirati daljnjim razvojem i prilagodbom svojih nacionalnih strategija za kibersigurnost. Od objave prvih studija ENISA-e povezanih s nacionalnom strategijom za kibersigurnost 2012. države članice EU-a i zemlje EFTA-e ostvarile su velik napredak u razvoju i provedbi svojih strategija.

U ovom se izvješću predstavlja rad ENISA-e na izradi okvira za procjenu nacionalnih kapaciteta (NCAF).

Cilj je okvira državama članicama pružiti samoprocjenu njihove razine zrelosti ocjenjivanjem ciljeva nacionalnih strategija za kibersigurnost, što će im pomoći u jačanju i izgradnji kibersigurnosnih kapaciteta na strateškoj i operativnoj razini.

U njemu se iznosi jednostavan reprezentativni prikaz razine zrelosti kibersigurnosti u državi članici. Okvir za procjenu nacionalnih kapaciteta alat je koji državama članicama pomaže:

- pružiti korisne informacije za razvoj dugoročne strategije (npr. dobru praksu, smjernice);
- pri utvrđivanju elemenata koji nedostaju u okviru nacionalne strategije za kibersigurnost;
- u daljnjem jačanju kapaciteta
- podržavanjem odgovornosti za politička djelovanja;
- osigurati vjerodostojnost u široj javnosti i među međunarodnim partnerima;
- pri informiranju javnosti i stvaranju boljeg dojma u javnosti o transparentnosti organizacije;
- predvidjeti buduće probleme;
- utvrditi stečena iskustva i najbolje prakse;
- osigurati osnove za kapacitete u području kibersigurnosti u cijelom EU-u kako bi se olakšale rasprave i
- u ocjenjivanju nacionalnih kapaciteta u području kibersigurnosti.

Taj je okvir osmišljen uz potporu stručnjaka za predmetno područje ENISA-e i predstavnika iz 19 država članica i zemalja EFTA-e[1]. Ciljna su publika ovog izvješća tvorci politika, stručnjaci i državni dužnosnici odgovorni za osmišljavanje, provedbu i procjenu nacionalne strategije za kibersigurnost ili uključeni u te postupke i, na široj razini, kapaciteta u području kibersigurnosti.

[1]Obavljeni su razgovori s predstavnicima sljedećih država članica i zemalja EFTA-e: Belgijom, Češkom, Danskom, Estonijom, Grčkom, Hrvatskom, Irskom, Italijom, Lihtenštajnom, Mađarskom, Maltom, Nizozemskom, Norveškom, Portugalom, Slovačkom, Slovenijom, Španjolskom, Švedskom.

Okvirom za procjenu nacionalnih kapaciteta obuhvaćeno je 17 strateških ciljeva koji su strukturirani oko četiri glavna klastera:

- Klaster br. 1: Upravljanje i norme u području kibersigurnosti
  1. Izrada nacionalnog plana za nepredvidive situacije u području kibersigurnosti
  2. Utvrđivanje osnovnih sigurnosnih mjera
  3. Siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge

- Klaster br. 2: Izgradnja kapaciteta i podizanje svijesti
  4. Organizacija vježbi u području kibersigurnosti
  5. Uspostava kapaciteta odgovora na incidente
  6. Podizanje svijesti korisnika
  7. Jačanje programa osposobljavanja i izobrazbe
  8. Poticanje istraživanja i razvoja
  9. Poticanje privatnog sektora na ulaganje u sigurnosne mjere
  10. Poboljšanje kibersigurnosti lanca opskrbe

- Klaster br. 3: Pravna i regulatorna pitanja
  11. Zaštita ključne informatičke infrastrukture, operatora ključnih usluga i pružatelja digitalnih usluga
  12. Borba protiv kiberkriminaliteta
  13. Uspostava mehanizama za izvješćivanje o incidentima
  14. Jačanje privatnosti i zaštite podataka

- Klaster br. 4: Suradnja
  15. Uspostava javno-privatnog partnerstva
  16. Institucionalizacija suradnje javnih agencija
  17. Sudjelovanje u međunarodnoj suradnji

1. UVOD

Direktivom o mrežnoj i informacijskoj sigurnosti (NIS), objavljenom u srpnju 2016., od država članica EU-a zahtijeva se da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava, koja se naziva i NCSS (nacionalna strategija za kibersigurnost), kako je utvrđeno u člancima 1. i 7. U tom se kontekstu nacionalna strategija za kibersigurnost definira kao okvir kojim se utvrđuju strateška načela, smjernice, strateški ciljevi, prioriteti, odgovarajuće politike i regulatorne mjere. Predviđeni je cilj nacionalne strategije za kibersigurnost postizanje i održavanje visoke razine sigurnosti mreža i sustava, čime se državama članicama omogućuje da ublaže potencijalne prijetnje. Osim toga, nacionalna strategija za kibersigurnost ujedno može biti katalizator industrijskog razvoja te gospodarskog i društvenog napretka.

U Aktu EU-a o kibersigurnosti navodi se da ENISA promiče širenje najboljih praksi u definiranju i provedbi nacionalne strategije za kibersigurnost pružanjem potpore državama članicama u donošenju Direktive NIS i prikupljanjem vrijednih povratnih informacija o njihovim iskustvima. U tu je svrhu ENISA razvila nekoliko alata kako bi pomogla državama članicama u razvoju, provedbi i ocjenjivanju njihovih nacionalnih strategija za kibersigurnost.

ENISA u okviru svojeg mandata nastoji razviti okvir za samoprocjenu nacionalnih kapaciteta kako bi se izmjerila razina zrelosti različitih nacionalnih strategija za kibersigurnost. Cilj je ovog izvješća predstaviti studiju provedenu u okviru definiranja okvira za samoprocjenu.

1.1 OPSEG I CILJEVI STUDIJE

Glavni je cilj ove studije uspostaviti okvir za samoprocjenu nacionalnih kapaciteta (NCAF) kako bi se izmjerila razina zrelosti u području kibersigurnosti u državama članicama. Konkretnije, okvirom bi se države članice trebale osnažiti u:

- provedbi procjene nacionalnih kapaciteta u području kibersigurnosti;
- podizanju svijesti o razini zrelosti pojedine zemlje;
- utvrđivanju područja u kojima su potrebna poboljšanja i
- jačanju kapaciteta u području kibersigurnosti.

Taj bi okvir trebao pomoći državama članicama, posebno nacionalnim tvorcima politika, da provedu samoprocjenu u cilju poboljšanja nacionalnih kapaciteta u području kibersigurnosti.

1.2 METODOLOŠKI PRISTUP

Metodološki pristup korišten za razvoj okvira za samoprocjenu nacionalnih kapaciteta oslanja se na četiri glavna koraka, koji su:

1. **Analiza dokumentacije**: Prvi korak uključivao je provedbu opsežnog pregleda literature kako bi se prikupile najbolje prakse u pogledu razvoja okvira za ocjenjivanje zrelosti nacionalnih strategija kibersigurnosti. Analiza dokumentacije usmjerena je na sustavnu analizu relevantnih dokumenata o izgradnji kapaciteta u području kibersigurnosti i definiranju strategije, na postojeće nacionalne strategije za kibersigurnost država članica i na usporedbu postojećih modela zrelosti u području kibersigurnosti. Utvrđivanje referentnih vrijednosti za postojeće modele zrelosti provedeno je donošenjem okvira analize izrađenog za potrebe ove studije. Okvir

analize temelji se na Beckerovoj[2] metodologiji za razvoj modela zrelosti kojom se utvrđuje opći i konsolidirani model postupka za izradu modela zrelosti i pružaju jasni zahtjevi za razvoj modela zrelosti. Okvir analize dodatno je prilagođen kako bi se zadovoljile potrebe ove studije.

2. **Prikupljanje mišljenja stručnjaka i dionika**: Na temelju podataka prikupljenih analizom dokumentacije i povezanih preliminarnih nalaza analize, ta faza obuhvaćala je utvrđivanje i pozivanje na razgovore stručnjaka koji imaju iskustva u razvoju i provedbi nacionalnih strategija za kibersigurnost ili modela zrelosti. ENISA se obratila svojoj Skupini stručnjaka za nacionalne strategije kibersigurnosti i nacionalnim časnicima za vezu kako bi pronašla relevantne stručnjake u svakoj državi članici. Osim toga, obavljeni su razgovori s nekim stručnjacima uključenima u razvoj modela zrelosti. Ukupno su obavljena 22 razgovora, od kojih 19 s predstavnicima agencija za kibersigurnost iz različitih država članica (i zemalja EFTA-e).
3. **Analiza ulaznih podataka za pregled stanja:** Podatci prikupljeni analizom dokumentacije i razgovorima naknadno su analizirani u cilju utvrđivanja najbolje prakse u izradi okvira za samoprocjenu kako bi se izmjerila zrelost nacionalnih strategija za kibersigurnost, razumjele potrebe država članica i utvrdilo koji se podatci mogu lako prikupiti u različitim europskim zemljama[3]. Tom je analizom omogućena prilagodba preliminarnog modela razvijenog u prethodnim koracima i poboljšanje skupa pokazatelja uključenih u model, razina zrelosti i njegovih dimenzija.
4. **Dovršavanje modela:** Nakon toga relevantni stručnjaci ENISA-e pregledali su ažuriranu verziju okvira za samoprocjenu nacionalnih kapaciteta te su ih zatim dodatno potvrdili stručnjaci na radionici održanoj u listopadu 2020. prije objave.

1.3 CILJNA PUBLIKA

Ciljna su publika ovog izvješća tvorci politika, stručnjaci i državni dužnosnici odgovorni za osmišljavanje, provedbu i procjenu nacionalne strategije za kibersigurnost ili uključeni u te postupke i, na široj razini, kapaciteta u području kibersigurnosti. Osim toga, nalazi koji su formalizirani u ovom dokumentu mogu biti korisni stručnjacima za politiku kibersigurnosti i istraživačima na nacionalnoj ili europskoj razini.

[2] J. Becker, R. Knackstedt i J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, svezak 1., br. 3, str. 213. – 222., lipanj 2009.
[3] Za potrebe tog istraživanja „europske zemlje" na koje se upućuje u ovom izvješću uključuju 27 država članica EU-a.

2. KONTEKST

2.1 PRETHODNI RAD NA ŽIVOTNOM CIKLUSU NACIONALNE STRATEGIJE ZA KIBERSIGURNOST

Kako je navedeno u Aktu EU-a o kibersigurnosti, jedan od glavnih ciljeva ENISA-e jest pružanje potpore državama članicama u razvoju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava, promicanje širenja tih strategija i praćenje njihove provedbe. ENISA je u okviru svojeg mandata izradila nekoliko dokumenata o toj temi kako bi se potaknula razmjena dobrih praksi i podržala provedba nacionalnih strategija za kibersigurnost diljem EU-a:

- Praktični vodič kroz fazu razvoja i provedbe nacionalne strategije za kibersigurnost[4] objavljen 2012.
- Dokument Utvrđivanje smjera nacionalnih napora za jačanje sigurnosti u kiberprostoru[5] objavljen 2012.
- Prvi okvir ENISA-e za procjenu nacionalne strategije za kibersigurnost neke države članice[6] objavljen 2014.
- Interaktivna internetska karta nacionalnih strategija za kibersigurnost[7] objavljena 2014.
- Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost[8] objavljen 2016.
- Alat za procjenu nacionalnih strategija za kibersigurnost[9] objavljen 2018.
- Dokument Dobre prakse u inovacijama u području kibersigurnosti u okviru nacionalne strategije za kibersigurnost[10] objavljen 2019.

PRILOG A sadržava kratak sažetak glavnih publikacija ENISA-e o toj temi.

Navedeni vodiči i dokumenti proučavani su u okviru analize dokumentacije. Konkretno, Nacionalni alat za procjenu strategija za kibersigurnost[11] temeljni je element okvira za procjenu nacionalnih kapaciteta. Okvir za procjenu nacionalnih kapaciteta temelji se na ciljevima obuhvaćenima internetskim alatom za procjenu nacionalnih strategija za kibersigurnost.

[4] Nacionalna strategija za kibersigurnost: Praktični vodič kroz razvoj i izvršenje (ENISA, 2012.)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] Nacionalna strategija za kibersigurnost: Utvrđivanje smjera nacionalnih napora za jačanje sigurnosti u kiberprostoru (ENISA, 2012.)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] Okvir za procjenu nacionalne strategije za kibersigurnost (ENISA, 2014.)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Nacionalne strategije za kibersigurnost – interaktivna karta (ENISA, 2014., ažurirana 2019.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Ovim se dokumentom ažurira vodič iz 2012.: Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost: Osmišljavanje i provedba nacionalnih strategija za kibersigurnost (ENISA, 2016.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] Alat za procjenu nacionalnih strategija za kibersigurnost (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] Alat za procjenu nacionalnih strategija za kibersigurnost (2018.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 ZAJEDNIČKI CILJEVI UTVRĐENI U OKVIRU EUROPSKE NACIONALNE STRATEGIJE ZA KIBERSIGURNOST

Razlike među državama članica otežavaju utvrđivanje zajedničkih aktivnosti ili akcijskih planova u različitim nacionalnim kontekstima, pravnim okvirima i političkim programima. Međutim, strateški ciljevi nacionalnih strategija za kibersigurnost država članica često se temelje na istim temama. Stoga su na temelju prethodnog rada ENISA-e i analize nacionalnih strategija za kibersigurnost država članica utvrđena 22 strateška cilja. U prethodnom radu ENISA-e već je utvrđeno 15 od tih strateških ciljeva, dva su nova cilja dodana u ovoj studiji te je utvrđeno pet ciljeva za buduća razmatranja.

2.2.1 Zajednički strateški ciljevi koje su prihvatile države članice

Na temelju prethodnog rada ENISA-e, odnosno alata za ocjenjivanje nacionalnih strategija za kibersigurnost,[12] u tablici u nastavku prikazan je prethodno navedeni skup od 15 strateških ciljeva koji su zajednički obuhvaćeni nacionalnim strategijama za kibersigurnost država članica. Ciljevi opisuju srž cjelokupne „nacionalne filozofije" o toj temi. Dodatne informacije o ciljevima opisanima u nastavku potražite u izvješću ENISA-e Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost.[13]

Tablica 1.: Zajednički strateški ciljevi koje su države članice obuhvatile svojim nacionalnim strategijama za kibersigurnost

Oznaka	Strateški ciljevi nacionalne strategije za kibersigurnost	Ciljevi
1	Razvoj nacionalnih planova za nepredvidive situacije u području kibersigurnosti	▶ predstaviti i objasniti kriterije na temelju kojih bi se situacija definirala kao kriza ▶ utvrditi ključne postupke i mjere za rješavanje krize ▶ jasno definirati uloge i odgovornosti različitih dionika tijekom kiberkrize ▶ predstaviti i objasniti kriterije za okončanje krize i tko je to ovlašten proglasiti
2	Utvrđivanje osnovnih sigurnosnih mjera	▶ uskladiti različite prakse organizacija u javnom i privatnom sektoru ▶ stvoriti zajednički jezik između nadležnih javnih tijela i organizacija te uspostaviti sigurne komunikacijske kanale ▶ omogućiti različitim dionicima da provjere i usporede svoje kapacitete u području kibersigurnosti ▶ razmjenjivati informacije o dobroj praksi u području kibersigurnosti u svakom industrijskom sektoru ▶ pomoći dionicima da odrede prioritete svojih ulaganja u području sigurnosti
3	Organizacija vježbi u području kibersigurnosti	▶ utvrditi što treba ispitati (planovi i procesi, ljudi, infrastruktura, kapaciteti za odgovor, sposobnosti suradnje, komunikacija itd.) ▶ uspostaviti nacionalni tim za planiranje kibervježbi s jasnim mandatom ▶ integracija kibervježbi u životni ciklus nacionalne strategije za kibersigurnost ili nacionalnog plana nepredvidive situacije u području kibersigurnosti
4	Uspostava sposobnosti odgovora na incidente	▶ mandat – odnosi se na ovlasti, uloge i odgovornosti koje predmetna vlada treba dodijeliti timu ▶ portfelj usluga – obuhvaća usluge koje tim pruža svojoj jedinici ili koristi za vlastito unutarnje funkcioniranje

[12] Alat za procjenu nacionalnih strategija za kibersigurnost (2018.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Ovim se dokumentom ažurira vodič iz 2012.: Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost: Osmišljavanje i provedba nacionalnih strategija za kibersigurnost (ENISA, 2016.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Oznaka	Strateški ciljevi nacionalne strategije za kibersigurnost	Ciljevi
		▶ operativni kapaciteti – odnose se na tehničke i operativne zahtjeve koje tim mora ispunjavati ▶ sposobnosti za suradnju – obuhvaćaju zahtjeve u pogledu razmjene informacija s drugim timovima koji nisu obuhvaćeni prethodnim trima kategorijama, npr. tvorcima politika, vojskom, regulatornim tijelima, operatorima (ključne informatičke infrastrukture), tijelima za izvršavanje zakonodavstva
5	Podizanje svijesti korisnika	▶ utvrditi nedostatke u znanju o kibersigurnosti ili pitanjima informacijske sigurnosti ▶ ukloniti razlike podizanjem razine svijesti ili razvojem/jačanjem temeljâ znanja
6	Jačanje programa osposobljavanja i izobrazbe	▶ poboljšati operativne kapacitete postojeće radne snage u području informacijske sigurnosti ▶ poticati učenike da se pridruže i zatim ih pripremiti za ulazak u područje kibersigurnosti ▶ promicati i poticati odnose između akademskog okruženja informacijske sigurnosti i industrije informacijske sigurnosti ▶ uskladiti osposobljavanje u području kibersigurnosti s poslovnim potrebama
7	Poticanje istraživanja i razvoja	▶ utvrditi stvarne uzroke ranjivosti umjesto otklanjanja njihova učinka ▶ okupiti znanstvenike iz različitih disciplina kako bi se pronašla rješenja za višedimenzionalne i složene probleme kao što su fizičke kiberprijetnje ▶ objediniti potrebe industrije i rezultate istraživanja, čime se olakšava prelazak iz teorije u praksu ▶ pronaći načine ne samo za održavanje, već i za povećanje razine kibersigurnosti proizvoda i usluga kojima se podržava postojeću kiberinfrastrukturu
8	Poticanje privatnog sektora na ulaganje u sigurnosne mjere	▶ utvrditi moguće poticaje za privatna poduzeća da ulažu u sigurnosne mjere ▶ pružiti poticaje poduzećima za promicanje ulaganja u sigurnost
9	Zaštita ključne informatičke infrastrukture (CII), operatora ključnih usluga i pružatelja digitalnih usluga	▶ utvrditi ključnu informatičku infrastrukturu ▶ utvrditi i ublažiti relevantne rizike za ključnu informatičku infrastrukturu
10	Borba protiv kiberkriminaliteta	▶ donijeti zakone u području kiberkriminaliteta ▶ povećati djelotvornost agencija za izvršavanje zakonodavstva
11	Uspostava mehanizama za izvješćivanje o incidentima	▶ stjecanje znanja o cjelokupnom okruženju prijetnji ▶ procijeniti učinak incidenata (npr. povrede sigurnosti, kvarovi mreže, prekidi usluga) ▶ stjecanje znanja o postojećim i novim oblicima ranjivosti i vrstama napada ▶ u skladu s tim ažurirati sigurnosne mjere ▶ provesti odredbe Direktive NIS o izvješćivanju o incidentima
12	Jačanje privatnosti i zaštite podataka	▶ doprinijeti jačanju temeljnih prava na privatnost i zaštitu podataka
13	Uspostava javno-privatnog partnerstva (JPP);	▶ odvraćanje (kako se napadače ne bi motiviralo) ▶ zaštita (upotreba istraživanja u pogledu novih sigurnosnih prijetnji); ▶ otkrivanje (razmjena informacija radi otklanjanja novih prijetnji); ▶ odgovor (kako bi se osigurala sposobnost suočavanja s početnim učinkom incidenta) ▶ oporavak (kako bi se osigurala sposobnost popravka konačnog učinka incidenta)
14	Institucionalizacija suradnje javnih agencija	▶ povećati suradnju između javnih agencija s odgovornostima i kompetencijama povezanima s kibersigurnošću ▶ izbjeći preklapanje nadležnosti i resursa između javnih agencija

Oznaka	Strateški ciljevi nacionalne strategije za kibersigurnost	Ciljevi
		▶ poboljšati i institucionalizirati suradnju među javnim agencijama u različitim područjima kibersigurnosti
15	Sudjelovanje u međunarodnoj suradnji (ne samo s državama članicama EU-a)	▶ ostvariti koristi od uspostave zajedničke baze znanja među državama članicama EU-a ▶ stvoriti sinergijske učinke među nacionalnim tijelima za kibersigurnost ▶ omogućiti i ojačati borbu protiv transnacionalnog kriminala

2.2.2 Dodatni strateški ciljevi

Na temelju obavljene analize dokumentacije i razgovora koje je provela ENISA utvrđeni su dodatni strateški ciljevi. Države članice sve se više bave tim temama u svojim nacionalnim strategijama za kibersigurnost ili definiraju akcijske planove o toj temi. Navedeni su i primjeri aktivnosti koje provode države članice. Ako je primjer iz javno dostupnog izvora, upućuje se na njega. U slučajevima u kojima se primjeri temelje na povjerljivim razgovorima s dužnosnicima država članica EU-a ne navode se upućivanja.

Utvrđeni su sljedeći dodatni strateški ciljevi:

- poboljšanje kibersigurnosti lanca opskrbe i
- siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge.

Poboljšanje kibersigurnosti lanca opskrbe

Mala i srednja poduzeća (MSP-ovi) okosnica su europskoga gospodarstva. Čine 99 % svih poduzeća u EU-u,[14] a 2015. godine procijenjeno je da su MSP-ovi otvorili oko 85 % novih radnih mjesta i osigurali dvije trećine ukupnog broja radnih mjesta u privatnom sektoru u EU-u. Nadalje, s obzirom na to da MSP-ovi pružaju usluge velikim poduzećima i sve više surađuju s javnom upravom,[15] potrebno je napomenuti da su u današnjem međusobno povezanom kontekstu MSP-ovi slaba karika kibernapada. Naime, MSP-ovi su najizloženiji kibernapadima, ali si često ne mogu priuštiti odgovarajuća ulaganja u kibersigurnost.[16] Stoga bi poboljšanje kibersigurnosti lanca opskrbe trebalo provoditi s naglaskom na MSP-ovima.

Osim tog sustavnog pristupa, države članice mogu staviti naglasak i na kibersigurnost određenih usluga i proizvoda IKT-a koji se smatraju ključnima: Informacijska i komunikacijska tehnologija koja se upotrebljava u okviru ključne informatičke infrastrukture, sigurnosni mehanizmi koji se primjenjuju u telekomunikacijskom sektoru (kontrole na razini pružatelja internetskih usluga..), usluge povjerenja kako su definirane u Uredbi eIDAS i pružatelji usluga računalstva u oblaku. Na primjer, Poljska se u svojoj nacionalnoj strategiji za kibersigurnost[17] za razdoblje 2019. – 2024. obvezala razviti nacionalni sustav kibersigurnosne procjene i certifikacije kao mehanizam za osiguranje kvalitete u lancu opskrbe. Taj sustav certifikacije bit će usklađen s certifikacijskim okvirom EU-a za digitalne proizvode, usluge i procese IKT-a uspostavljenim Aktom EU-a o kibersigurnosti (2019/881).

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

Stoga je poboljšanje kibersigurnosti lanca opskrbe od ključne važnosti. To se može postići uspostavom snažnih politika za promicanje MSP-ova, pružanjem smjernica za zahtjeve u pogledu kibersigurnosti u postupcima javne nabave, poticanjem suradnje u privatnom sektoru, uspostavom javno-privatnih partnerstava, promicanjem mehanizama koordiniranog otkrivanja ranjivosti (CVD),[18] programom za certifikaciju proizvoda, uključujući komponente kibersigurnosti u digitalnim inicijativama za MSP-ove, te, među ostalim, financiranjem razvoja vještina.

Siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge
Komisija je u veljači 2020. iznijela svoju viziju digitalne transformacije EU-a u Komunikaciji „Izgradnja digitalne budućnosti Europe"[19] s ciljem izgradnje uključivih tehnologija koje su u interesu građana i kojima se poštuju temeljne vrijednosti EU-a. Konkretno, u Komunikaciji se navodi da je promicanje digitalne transformacije javnih uprava u cijeloj Europi od ključne važnosti. U tom je smislu od iznimne važnosti izgradnja povjerenja u vladu u pogledu digitalnog identiteta i povjerenja u javne usluge. To je još važnije kada se uzme u obzir činjenica da su transakcije i razmjene podataka u javnom sektoru često osjetljive prirode.

Mnoge su zemlje izrazile namjeru da razmotre tu temu u svojim nacionalnim strategijama za kibersigurnost, kao što su: Danska, Estonija, Francuska, Luksemburg, Malta, Španjolska, Nizozemska i Ujedinjena Kraljevina. Neke od tih zemalja navele su i da bi se taj strateški cilj mogao ostvariti u okviru šireg plana:

- Estonija povezuje svoj akcijski plan „Sigurnost elektroničkog identiteta i sposobnost elektroničke autentifikacije" sa širom Digitalnom agendom za 2020. za Estoniju.
- U francuskoj nacionalnoj strategiji za kibersigurnost navodi se da državni tajnik odgovoran za digitalnu tehnologiju nadgleda uspostavu plana „za zaštitu digitalnih života, privatnosti i osobnih podataka francuskog naroda".
- U nizozemskoj nacionalnoj strategiji za kibersigurnost navodi se da se o kibersigurnosti u javnim upravama, kao i o javnim uslugama koje se pružaju građanima i poduzećima, detaljnije raspravlja u opsežnom programu za digitalnu upravu.
- Budući da vlada Ujedinjene Kraljevine nastavlja širiti svoje usluge na internetu, uspostavila je Državnu digitalnu službu (GDS), koja osigurava da sve nove digitalne usluge koje je pokrenula ili nabavila vlada imaju „zadanu sigurnost" (engl. secure by default), uz potporu Britanskog nacionalnog centra za kibersigurnost (NCSC).

2.2.3 Ostali razmatrani strateški ciljevi

Tijekom faze analize dokumentacije i u okviru razgovora koje je vodila ENISA proučavani su drugi strateški ciljevi. No odlučeno je da ti ciljevi neće biti dio okvira za samoprocjenu. PRILOG C – Ostali analizirani ciljevi

U njima se navode definicije za svaki od tih ciljeva koje se mogu upotrijebiti za poticanje budućih rasprava o mogućim poboljšanjima nacionalne strategije za kibersigurnost.

Kao buduća razmatranja ispitivali su se sljedeći ciljevi:

- razvoj sektorskih strategija za kibersigurnost;
- borba protiv kampanja dezinformiranja;
- sigurne najsuvremenije tehnologije (5G, umjetna inteligencija, kvantno računalstvo...);
- osiguravanje suvereniteta nad podatcima i

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

- pružanje poticaja za razvoj industrije kiberosiguranja.

2.3 KLJUČNI ZAKLJUČCI IZ POSTUPKA UTVRĐIVANJA REFERENTNIH VRIJEDNOSTI

Analiza dokumentacije o postojećim modelima zrelosti povezanima s kibersigurnošću provedena je s ciljem prikupljanja informacija i dokaza kako bi se podržalo osmišljavanje okvira za samoprocjenu nacionalnih kapaciteta u području nacionalnih strategija za kibersigurnost. U tom je kontekstu proveden opsežan pregled literature o postojećim modelima kako bi se dopunili nalazi početnog istraživanja opsega modela zrelosti kibersigurnosti i postojeće nacionalne strategije za kibersigurnost, koji su razrađeni u odjeljcima 2.1 i 2.2. Tim se sustavnim preispitivanjem podržavaju odabir i obrazloženje razina zrelosti okvira za procjenu te definicija različitih dimenzija i pokazatelja.

U okviru sustavnog preispitivanja modela zrelosti razmatrano je i analizirano 10 modela na temelju njihovih ključnih značajki. Opći pregled ključnih značajki svakog modela preispitanog u okviru ove studije dostupan je u tablici 2.: Pregled analiziranih modela zrelosti a detaljnija analiza nalazi se u PRILOGU A.

Tablica 2.: Pregled analiziranih modela zrelosti

Naziv modela	Razina zrelosti	Broj atributa	Metoda procjene	Prikaz rezultata
Model zrelosti kapaciteta u području kibersigurnosti za države (CMM)	5	5 glavnih dimenzija	Suradnja s lokalnom organizacijom radi prilagodbe modela prije njegove primjene u nacionalnom kontekstu	Radar s pet odjeljaka
Model zrelosti kapaciteta u području kibersigurnosti (C2M2)	4	10 glavnih domena	Metodologija i skup alata za samoocjenjivanje	Bodovna kartica s kružnim grafikonima
Okvir za poboljšanje kibersigurnosti ključne infrastrukture	Nije primjenjivo (4 reda)	5 osnovnih funkcija	Samoprocjena	Nije primjenjivo
Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2)	5	5 glavnih domena	Nije primjenjivo	Nije primjenjivo
Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)	5	17 glavnih domena	Procjena koju provode revizori treće strane	Nije primjenjivo
Model zrelosti kibersigurnosti zajednice (CCSMM)	5	6 glavnih dimenzija	Procjena unutar zajednica uz doprinos državnih i saveznih agencija za izvršavanje zakonodavstva	Nije primjenjivo
Model zrelosti informacijske sigurnosti za okvir kibersigurnosti NIST-a (ISMM)	5	23 ocijenjena područja	Nije primjenjivo	Nije primjenjivo
Model sposobnosti unutarnje revizije (IA-CM) za javni sektor	5	6 elemenata	Samoprocjena	Nije primjenjivo
Globalni indeks kibersigurnosti (GCI)	NIJE PRIMJENJIVO	5 stupova	Samoprocjena	Rang-lista
Indeks kibersposobnosti (CPI)	NIJE PRIMJENJIVO	4 kategorije	Komparativna analiza koju provodi jedinica Economist Intelligence Unit	Rang-lista

Tim sustavnim preispitivanjem omogućeno je donošenje zaključaka o najboljim praksama usvojenima u postojećim modelima kako bi se podržao razvoj konceptualnog modela za postojeći model zrelosti. Konkretno, u okviru postupka utvrđivanja referentnih vrijednosti podržava se definicija razina zrelosti, stvaranje klastera dimenzija i odabir pokazatelja te odgovarajuća metodologija vizualizacije rezultata modela. Najrelevantniji nalazi za svaki od tih elemenata detaljno su opisani u tablici 3.

Tablica 3.: Ključni zaključci iz postupka utvrđivanja referentnih vrijednosti

Značajka	Ključni zaključak
Razine zrelosti	▶ ljestvica zrelosti od pet razina za okvire za ocjenjivanje kapaciteta u području kibersigurnosti opće je prihvaćena i u okviru nje mogu se dobiti detaljni rezultati procjene (vidjeti Tablicu 6. : Usporedba razina zrelost za iscrpan pregled definicije razina zrelosti za svaki model); ▶ svi modeli pružaju definiciju na visokoj razini za svaku razinu zrelosti koja se zatim prilagođava različitim dimenzijama ili klasterima dimenzija; ▶ pri mjerenju zrelosti kapaciteta u području kibersigurnosti obično se procjenjuju dva glavna aspekta: zrelost strategija i zrelost postupaka uspostavljenih za provedbu strategija
Atributi	▶ komparativna analiza atributa postojećih modela zrelosti pokazuje heterogene rezultate s prosječnim brojem atributa po modelu od četiri do pet; ▶ model koji se oslanja na oko 4 ili 5 atributa pruža zemljama odgovarajuću razinu granularnosti podataka grupiranjem relevantnih dimenzija i osiguravanjem čitljivosti rezultata (vidjeti Tablicu 7.: Usporedba atributa/**dimenzija** za opis atributa za svaki model); ▶ ključno načelo koje su svi modeli prihvatili pri definiranju klastera temelji se na dosljednosti elementa grupiranog u svakom klasteru
Metoda procjene	▶ metode procjene korištene u različitim analiziranim modelima međusobno se razlikuju; ▶ najčešća metoda procjene temelji se na samoprocjeni
Prikaz rezultata	▶ važno je predstaviti rezultate na različitoj razini granularnosti; ▶ metodologija vizualizacije trebala bi biti razumljiva sama po sebi i jednostavna za čitanje

Konceptualni model temeljio se na komparativnoj analizi različitih modela zrelosti, kao i na prethodnom radu ENISA-e. Osim toga, odlučeno je da će se na temelju internetskog interaktivnog alata ENISA-e razviti pokazatelji zrelosti koji se upotrebljavaju za svaki atribut.

2.4 IZAZOVI PRI PROCJENI NACIONALNE STRATEGIJE ZA KIBERSIGURNOST

Države članice suočavaju se s brojnim izazovima pri izgradnji kapaciteta u području kibersigurnosti i, konkretnije, pri osiguravanju da su njihovi kapaciteti u skladu s najnovijim kretanjima. U nastavku se nalazi sažetak izazova koje su utvrdile države članice i o kojima se s njima raspravljalo u okviru ove studije:

- **poteškoće u koordinaciji i suradnji:** koordinacija napora u području kibersigurnosti na nacionalnoj razini radi učinkovitog odgovora na pitanja kibersigurnosti može se pokazati izazovom zbog velikog broja uključenih dionika;
- **nedostatak sredstava za provedbu procjene:** ovisno o lokalnom kontekstu i strukturi nacionalnog upravljanja u području kibersigurnosti, ocjenjivanje nacionalne strategije za kibersigurnost i njezinih ciljeva može obuhvaćati više od 15 dana/osoba;
- **nedostatak potpore za razvoj kapaciteta u području kibersigurnosti:** neke države članice složile su se da, kako bi obranile proračun i dobile potporu za razvoj kapaciteta u području kibersigurnosti, prvo moraju provesti fazu procjene kako bi utvrdile nedostatke i ograničenja;
- **poteškoće u pripisivanju uspjeha ili promjena u strategiji:** s obzirom na to da se prijetnje svakodnevno razvijaju, a tehnologija poboljšava, kao odgovor na njih potrebno je stalno prilagođavati akcijske planove. Međutim, procjena nacionalne strategije za kibersigurnost i pripisivanje promjena strategiji i dalje je teška zadaća. To pak otežava utvrđivanje ograničenja i nedostataka nacionalne strategije za kibersigurnost;

- **poteškoće u mjerenju djelotvornosti nacionalne strategije za kibersigurnost:** mogu se prikupljati parametri za mjerenje različitih područja, kao što su napredak, provedba, zrelost i djelotvornost. Iako je mjerenje napretka i provedbe relativno jednostavno u usporedbi s mjerenjem djelotvornosti, ona je i dalje smislenija za procjenu ishoda i učinaka nacionalne strategije za kibersigurnost. Na temelju razgovora koje je obavila ENISA velik broj država članica izjavio je da je kvantitativno mjerenje djelotvornosti nacionalne strategije za kibersigurnost važno, ali da predstavlja i vrlo zahtjevnu zadaću koja je u nekim slučajevima prilično nemoguća;
- **poteškoće u donošenju zajedničkog okvira:** države članice EU-a djeluju u različitim kontekstima u smislu politike, organizacija, kulture, strukture društva i zrelosti nacionalnih strategija za kibersigurnost. Neke države članice s kojima su obavljeni razgovori u okviru ove studije izjavile su da bi moglo biti teško braniti i koristiti jedinstveni okvir za samoprocjenu.

2.5 KORISTI OD NACIONALNE PROCJENE KAPACITETA

Od 2017. sve države članice EU-a imaju nacionalnu strategiju za kibersigurnost.[20] Iako je riječ o pozitivnom razvoju, važno je i da države članice mogu pravilno ocijeniti te nacionalne strategije za kibersigurnost, čime se stvara dodana vrijednost njihovu strateškom planiranju i provedbi.

Jedan je od ciljeva okvira za procjenu nacionalnih kapaciteta ocijeniti sposobnosti u području kibersigurnosti na temelju prioriteta utvrđenih u različitim nacionalnim strategijama za kibersigurnost. Temeljno se u okviru ocjenjuje razina zrelosti kibersigurnosnih kapaciteta država članica u područjima definiranima ciljevima nacionalne strategije za kibersigurnost. Stoga rezultati okvira podržavaju tvorce politika država članica u definiranju nacionalne strategije za kibersigurnost pružajući im informacije o trenutačnom stanju u zemlji.[21] Okvir za procjenu nacionalnih kapaciteta u konačnici je namijenjen za pomoć državama članicama u utvrđivanju područja poboljšanja i izgradnji kapaciteta.

Cilj je okvira državama članicama pružiti samoprocjenu njihove razine zrelosti ocjenjivanjem njihovih ciljeva nacionalne strategije za kibersigurnost koji će im pomoći u jačanju i izgradnji kapaciteta u području kibersigurnosti na strateškoj i operativnoj razini.

Praktičnijim pristupom, na temelju razgovora koje je ENISA provela s nekoliko agencija odgovornih za područje kibersigurnosti u različitim državama članicama, utvrđene su i istaknute sljedeće koristi okvira za procjenu nacionalnih kapaciteta:

- pružanje korisnih informacija za razvoj dugoročne strategije (npr. dobre prakse, smjernica);
- pomoć pri utvrđivanju elemenata koji nedostaju u okviru nacionalne strategije za kibersigurnost;
- pomoć u daljnjem jačanju kapaciteta u području kibersigurnosti;
- potpora odgovornosti za politička djelovanja;
- osiguravanje vjerodostojnosti u široj javnosti i među međunarodnim partnerima;
- podrška informiranju javnosti i poboljšanje dojma u javnosti kao transparentne organizacije;
- pomoć u predviđanju budućih problema;
- pomoć u utvrđivanju stečenih iskustava i najboljih praksi;

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

- osiguranje osnove za kapacitete u području kibersigurnosti u cijelom EU-u kako bi se olakšale rasprave i
- pomoć u ocjenjivanju nacionalnih kapaciteta u području kibersigurnosti.

3. METODOLOGIJA OKVIRA ZA PROCJENU NACIONALNIH KAPACITETA

3.1 OPĆA SVRHA

Glavni cilj okvira za procjenu nacionalnih kapaciteta jest mjerenje razine zrelosti kapaciteta **država članica** u području kibersigurnosti kako bi im se pružila potpora u provedbi procjene njihovih nacionalnih kapaciteta u području kibersigurnosti, podizanju svijesti o razini zrelosti zemlje, utvrđivanju područja za poboljšanje i izgradnji kapaciteta u području kibersigurnosti.

3.2 RAZINE ZRELOSTI

Okvir se temelji na **pet razina zrelosti** kojima se definiraju faze koje države članice moraju proći u izgradnji kibersigurnosnih kapaciteta u području obuhvaćenom svakim ciljem nacionalne strategije za kibersigurnost. Te razine predstavljaju razine zrelosti koje se povećavaju, a počinju od **1. razine**, pri čemu države članice nemaju jasno definiran pristup za izgradnju kapaciteta za kibersigurnost u područjima obuhvaćenima ciljevima nacionalne strategije za kibersigurnost te završavaju **5. razinom**, pri čemu je strategija izgradnje kapaciteta u području kibersigurnosti dinamična i prilagodljiva kretanjima u pogledu okoliša. U tablici 4. prikazana je ljestvica razina zrelosti uz opis svake razine.

Tablica 4: ENISA-ina ljestvica pet razina zrelosti okvira za procjenu nacionalnih kapaciteta

1. RAZINA – POČETNA / AD HOC	2. RAZINA – RANA DEFINICIJA	3. RAZINA – USPOSTAVA	4. RAZINA – OPTIMIZACIJA	5. RAZINA – PRILAGODLJIVOST
Država članica nema jasno definiran pristup izgradnji kapaciteta u području kibersigurnosti u područjima obuhvaćenima ciljevima nacionalne strategije za kibersigurnost. Međutim, u zemlji možda postoje neki opći ciljevi te su provedene neke studije (tehničke, političke, u pogledu politika) kako bi se poboljšali nacionalni kapaciteti.	Definiran je nacionalni pristup izgradnji kapaciteta u području obuhvaćenom ciljevima nacionalne strategije za kibersigurnost. Akcijski planovi ili aktivnosti za postizanje rezultata uspostavljeni su, ali u ranoj fazi. Osim toga, možda su utvrđeni i/ili uključeni aktivni dionici.	Povezani dionici jasno definiraju i podržavaju akcijski plan za izgradnju kapaciteta u području obuhvaćenom ciljevima nacionalne strategije za kibersigurnost. Prakse i aktivnosti provode se i primjenjuju ujednačeno na nacionalnoj razini. Aktivnosti su definirane i dokumentirane s jasnom raspodjelom resursa i upravljanjem te skupom rokova.	Akcijski plan redovito se ocjenjuje: utvrđeni su prioriteti plana, plan je optimiziran i održiv. Redovito se mjeri uspješnost aktivnosti izgradnje kapaciteta u području kibersigurnosti. Utvrđeni su čimbenici uspjeha, izazovi i nedostatci u provedbi aktivnosti.	Strategija izgradnje kapaciteta u području kibersigurnosti dinamična je i prilagodljiva. Stalna pozornost posvećena kretanjima u pogledu okoliša (tehnološki napredak, globalni sukobi, nove prijetnje...) potiče sposobnost brzog odlučivanja i sposobnost brzog djelovanja radi poboljšanja.

3.3 KLASTERI I SVEOBUHVATNA STRUKTURA OKVIRA ZA SAMOPROCJENU

Okvir za samoprocjenu ima **četiri klastera**: I. upravljanje i norme u području kibersigurnosti, II. izgradnja kapaciteta i podizanje svijesti, III. pravna i regulatorna pitanja i IV. suradnja. Svaki od tih klastera obuhvaća ključno tematsko područje za izgradnju kapaciteta u području kibersigurnosti u određenoj zemlji i sadržava skup različitih ciljeva koje bi države članice mogle uključiti u svoje nacionalne strategije za kibersigurnost. Konkretno:

- **(I) upravljanje i norme u području kibersigurnosti**: ovim se klasterom mjeri kapacitet država članica za uspostavu odgovarajućeg upravljanja, normi i dobre prakse u području kibersigurnosti. Tom se dimenzijom razmatraju različiti aspekti kiberobrane i otpornosti uz istodobnu podršku razvoju nacionalne industrije kibersigurnosti i izgradnji povjerenja u vlade;
- **(II) izgradnja kapaciteta i podizanje svijesti**: u okviru ovog klastera procjenjuje se kapacitet država članica za podizanje svijesti o kibersigurnosnim rizicima i prijetnjama te o tome kako ih ukloniti. Osim toga, tom se dimenzijom mjeri sposobnost zemlje da stalno razvija kapacitete u području kibersigurnosti i povećava ukupnu razinu znanja i vještina u tom području. Bavi se razvojem kibersigurnosnog tržišta i napretkom u istraživanju i razvoju kibersigurnosti. Taj klaster okuplja sve ciljeve kojima se postavljaju temelji za poticanje izgradnje kapaciteta;
- **(III) pravna i regulatorna pitanja**: ovim se klasterom mjeri sposobnost država članica da uspostave potrebne pravne i regulatorne instrumente za rješavanje i suzbijanje porasta kiberkriminaliteta i povezanih kiberincidenata te za zaštitu ključne informatičke infrastrukture. Osim toga, tom se dimenzijom procjenjuje i kapacitet država članica za uspostavu pravnog okvira za zaštitu građana i poduzeća, primjerice u slučaju postizanja ravnoteže između sigurnosti i privatnosti i
- **(IV) suradnja:** ovim se klasterom ocjenjuje suradnja i razmjena informacija među različitim skupinama dionika na nacionalnoj i međunarodnoj razini kao važan alat za bolje razumijevanje i odgovor na okruženje s prijetnjama koje se stalno mijenja.

U model su uključeni ciljevi koje obično donose države članice i koji su odabrani među ciljevima navedenima u odjeljku 2.2. Modelom se konkretno ocjenjuju sljedeći ciljevi:

- 1. razvoj nacionalnih planova za nepredvidive situacije u području kibersigurnosti (I.)
- 2. utvrđivanje osnovnih sigurnosnih mjera (I.)
- 3. siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge (I.)
- 4. uspostava sposobnosti odgovora na incidente (II.)
- 5. podizanje svijesti korisnika (II.)
- 6. organizacija vježbi u području kibersigurnosti (II.)
- 7. jačanje programa osposobljavanja i izobrazbe (II.)
- 8. poticanje istraživanja i razvoja (II.)
- 9. poticanje privatnog sektora na ulaganje u sigurnosne mjere (II.)
- 10. poboljšanje kibersigurnosti lanca opskrbe (II.)
- 11. zaštita ključne informatičke infrastrukture, operatora ključnih usluga i pružatelja digitalnih usluga (III.)
- 12. borba protiv kiberkriminaliteta (III.)
- 13. uspostava mehanizama za izvješćivanje o incidentima (III.)
- 14. jačanje privatnosti i zaštite podataka (III.)
- 15. institucionalizacija suradnje javnih agencija (IV.)
- 16. sudjelovanje u međunarodnoj suradnji (IV.)
- 17. uspostava javno-privatnog partnerstva (IV.)

Četiri klastera i temeljni ciljevi kombiniraju se u modelu kako bi se dobio cjelovit pristup zrelosti kapaciteta država članica u području kibersigurnosti. Slika 1. prikazuje sveobuhvatnu strukturu okvira za samoprocjenu i pokazuje na koji su način ti elementi, odnosno ciljevi, klasteri i okvir za samoprocjenu, povezani s procjenom uspješnosti zemlje.

Slika 1.: Struktura okvira za samoprocjenu

Za svaki cilj uključen u okvir za samoprocjenu postoji niz pokazatelja raspoređenih između pet razina zrelosti. Svaki se pokazatelj temelji na dihotomnom (da/ne) pitanju. Pokazatelj može biti potreban ili nepotreban.

3.4 MEHANIZAM OCJENJIVANJA

U **mehanizmu ocjenjivanja** okvira za samoprocjenu uzimaju se u obzir prethodno navedeni elementi i načela navedena u odjeljku 3.5. Zapravo, model pruža ocjenu na temelju vrijednosti dvaju parametara, odnosno **razine zrelosti** i **omjera pokrivenosti**. Svaki od tih parametara može se izračunati na različitim razinama: i. po cilju, ii. po klasteru ciljeva ili iii. ukupno.

Ocjene na razini ciljeva

Ocjena stupnja zrelosti daje pregled razine zrelosti i pokazuje koji su kapaciteti i prakse uspostavljeni. Ocjena stupnja zrelosti izračunava se kao najviša razina za koju je ispitanik ispunio sve zahtjeve (*tj. odgovor DA na sva potrebna pitanja*), uz to što je ispunio sve zahtjeve prethodnih razina zrelosti.

Omjer pokrivenosti pokazuje opseg pokrivenosti svih pokazatelja za koje je odgovor pozitivan, bez obzira na njihovu razinu. Riječ je o dodatnoj vrijednosti koja uzima u obzir sve pokazatelje kojima se mjeri cilj. Omjer pokrivenosti izračunava se kao omjer između ukupnog broja pitanja unutar cilja i broja pitanja za koja je odgovor pozitivan.

Važno je pojasniti da se za ostatak dokumenta riječ ***ocjena*** upotrebljava i za vrijednosti razine zrelosti i omjer pokrivenosti.

Slika 2. – Mehanizam ocjenjivanja po cilju omogućuje vizualizaciju mehanizma procjene opisanog u odjeljku 3.1 koji će se detaljnije objasniti u nastavku.

Slika 2.: Mehanizam ocjenjivanja prema cilju

Na *slici 2. prikazan je primjer izračuna razine zrelosti prema cilju. Valja napomenuti da ispitanik ispunio sve zahtjeve prve tri razine zrelosti te da je samo djelomično ispunio zahtjeve 4. razine. Stoga ocjena upućuje na to da je* ***razina zrelosti ispitanika 3. razina za cilj „organizacija vježbi u području kibersigurnosti"****.*

Međutim, u primjeru prikazanom na slici 2. u razini zrelosti cilja ne mogu se obuhvatiti informacije dobivene iz pokazatelja koji imaju pozitivnu ocjenu i koji se nalaze iznad 3. razine zrelosti. U tom slučaju omjer pokrivenosti može pružiti pregled svih elemenata koje je ispitanik proveo kako bi ostvario taj cilj, unatoč njegovoj stvarnoj razini zrelosti. U tom je slučaju omjer između ukupnog broja pitanja unutar cilja i broja pitanja za koja je odgovor pozitivan jednak 19/27, tj. ***vrijednost omjera pokrivenosti iznosi 70 %.***

Osim toga, kako bi se prilagodilo posebnostima država članica, a istodobno omogućio dosljedan pregled, ocjena se izračunava na temelju dvaju različitih uzoraka na razini klastera i na ukupnoj razini:

- **opće ocjene:**: jedan potpuni uzorak koji obuhvaća sve ciljeve uključene u klaster ili unutar ukupnog okvira (od 1 do 17);
- **specifične ocjene:** jedan specifični uzorak koji obuhvaća samo ciljeve koje je odabrala država članica (obično odgovaraju ciljevima iz nacionalne strategije za kibersigurnost određene zemlje) unutar klastera ili unutar ukupnog okvira.

Ocjene na razini klastera

Opća razina zrelosti svakog klastera izračunava se kao aritmetička sredina razine zrelosti svih ciljeva unutar tog klastera.

Specifična razina zrelosti svakog klastera izračunava se kao aritmetička sredina razine zrelosti ciljeva unutar tog klastera koje je država članica odlučila procijeniti (obično odgovara ciljevima iz nacionalne strategije za kibersigurnost određene zemlje).

Na primjer, na slici 1. prikazano je da se klaster (I.) upravljanje i norme u području kibersigurnosti sastoji od tri cilja. *Pod pretpostavkom da je ispitanik odabrao ocijeniti samo prva dva cilja, ali ne i treći, i pod pretpostavkom da prva dva cilja predstavljaju razinu zrelosti od 2 odnosno 4, onda je razina zrelosti klastera, uzimajući u obzir sve ciljeve, 2. razina (klaster (I.) opća razina zrelosti = (2 + 4)/3), dok je razina zrelosti klastera, uzimajući u obzir samo posebne ciljeve koje je odabrao ocjenjivač, 3. razina (specifična razina zrelosti klastera (I.) = (2 + 4)/2).*

Opći omjer pokrivenosti svakog klastera izračunava se kao omjer između ukupnog broja pitanja unutar klastera i broja pitanja na koja je odgovor pozitivan.

Posebni omjer pokrivenosti svakog klastera izračunava se kao omjer između ukupnog broja pitanja unutar klastera koja se odnose na ciljeve koje je država članica odlučila procijeniti (obično odgovaraju ciljevima koji su prisutni u nacionalnoj strategiji za kibersigurnost određene zemlje) i broja pitanja na koja je odgovor pozitivan.

Ocjene na ukupnoj razini

Ukupna opća razina zrelosti zemlje izračunava se kao aritmetička sredina razine zrelosti svih ciljeva unutar okvira, od 1 do 17.

Ukupna specifična razina zrelosti zemlje izračunava se kao aritmetička sredina razine zrelosti ciljeva unutar okvira koje je država članica odlučila procijeniti (obično odgovara ciljevima iz nacionalne strategije za kibersigurnost određene zemlje).

Ukupni opći omjer pokrivenosti zemlje izračunava se kao omjer između ukupnog broja pitanja u okviru svih ciljeva uključenih u okvir (od jednog do 17) i broja pitanja na koja je odgovor pozitivan.

Ukupni posebni omjer pokrivenosti zemlje izračunava se kao omjer između ukupnog broja pitanja unutar ciljeva unutar okvira koji je država članica odlučila procijeniti (obično odgovaraju ciljevima iz nacionalne strategije za kibersigurnost određene zemlje) i broja pitanja na koja je odgovor pozitivan.

Ispitanici za svaki pokazatelj mogu odabrati treću opciju „ne znam / nije primjenjivo”. U tom se slučaju pokazatelj isključuje iz ukupnog izračuna rezultata.

Razine zrelosti na razini klastera i ukupnoj razini izračunavaju se aritmetičkom sredinom kako bi se prikazao napredak između dviju procjena. Naime, alternativa koja se sastoji od izračunavanja klastera i ukupnih razina zrelosti kao stupnja zrelosti cilja s najmanjom zrelosti – iako je relevantna sa stajališta zrelosti – ne može uzeti u obzir napredak postignut u područjima obuhvaćenima drugim ciljevima.

Budući da su razina klastera i ukupna razina konsolidirane za potrebe izvješćivanja, odlučeno je da će se upotrijebiti aritmetička sredina. Za veću točnost upotrijebite ocjene na objektivnoj razini za potrebe izvješćivanja.

Na slici 3. u nastavku sažeto su prikazani mehanizmi ocjenjivanja na različitim razinama modela (cilj, klaster, ukupno).

Slika 3.: Mehanizam ukupnog ocjenjivanja

3.5 ZAHTJEVI ZA OKVIR ZA SAMOPROCJENU

Okvir za procjenu nacionalnih kapaciteta predstavljen u ovom odjeljku temelji se na potrebama koje su istaknule države članice te nizu zahtjeva navedenih u nastavku:

- država članica dobrovoljno uvodi okvir za procjenu nacionalnih kapaciteta kao okvir za samoprocjenu;
- cilj okvira za procjenu nacionalnih kapaciteta jest mjerenje kapaciteta država članica u području kibersigurnosti s obzirom na 17 ciljeva. No država članica može odabrati ciljeve u odnosu na koje želi provesti procjenu i ocijeniti samo podskup od 17 ciljeva;
- cilj okvira za samoprocjenu jest izmjeriti razinu zrelosti kapaciteta države članice u području kibersigurnosti;
- rezultati procjene ne objavljuju se osim ako država članica to ne odluči učiniti na vlastitu inicijativu;
- država članica može prikazati rezultate procjene predstavljanjem razine zrelosti kapaciteta zemlje u području kibersigurnosti, klastera ciljeva ili čak jednog cilja;
- svi su ocijenjeni ciljevi jednako relevantni u okviru procjene i stoga imaju jednaku važnost. To se odnosi i na pokazatelje koji se primjenjuju u okviru njega;
- država članica može pratiti napredak tijekom vremena.

Okvirom za samoprocjenu nastoji se pružiti potpora državama članicama u izgradnji kibersigurnosnih kapaciteta, što uključuje i niz preporuka ili smjernica za usmjeravanje europskih zemalja u poboljšanje njihove razine zrelosti.

Napomena: te su preporuke ili smjernice općenite i temelje se na publikacijama ENISA-e i iskustvima stečenima u drugim zemljama te će se ovisiti o rezultatima samoprocjene.

4. POKAZATELJI OKVIRA ZA PROCJENU NACIONALNIH KAPACITETA

4.1 POKAZATELJI IZ OKVIRA

U ovom su odjeljku predstavljeni ENISA-ini pokazatelji okvira za procjenu nacionalnih kapaciteta. Odjeljci u nastavku organizirani su prema klasterima.

Za svaki je klaster u tablici prikazan sveobuhvatan skup pokazatelja u obliku pitanja koja predstavljaju određenu razinu zrelosti. Upitnik je glavni instrument za samoprocjenu. Za svaki cilj potrebno je zabilježiti dva skupa pokazatelja:

- skup općih pitanja o zrelosti strategije (9 općih pitanja), označenih od „a” do „c” za svaku razinu zrelosti koji se ponavljaju za svaki cilj i
- skup pitanja o kapacitetima u području kibersigurnosti (319 pitanja o kapacitetima u području kibersigurnosti), označenih brojevima od „1” do „10” za svaku razinu zrelosti, specifičnih za područje obuhvaćeno predmetnim ciljem.

Svako je pitanje označeno oznakom (0 – 1) koja pokazuje je li riječ o potrebnom pokazatelju (1) ili pokazatelju koji nije potreban (0) za razinu zrelosti.

Svako se pitanje može identificirati s pomoću identifikacijskog broja koji se sastoji od:

- broja cilja;
- razine zrelosti i
- broja pitanja.

Na primjer, pitanje ID 1.2.4. četvrto je pitanje 2. razine zrelosti strateškog cilja (I.) „Razvoj nacionalnih planova za nepredvidive situacije u području kibersigurnosti”.

Potrebno je napomenuti da u cijelom upitniku pitanja obuhvaćaju nacionalnu razinu, osim ako je drukčije navedeno. U svim pitanjima zamjenica „vi” odnosi se na državu članicu na općenit način, ne odnosi se na pojedinca ili državno tijelo koje provodi procjenu.

Definicija svakog cilja nalazi se u poglavljima 2.2 – Zajednički ciljevi utvrđeni u okviru europske nacionalne strategije za kibersigurnost.

4.1.1 Klaster br. 1: Upravljanje i norme u području kibersigurnosti

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
1 – Razvoj nacionalnih planova za nepredvidive situacije u području kibersigurnosti	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li počeli raditi na izradi nacionalnih planova za nepredvidive situacije u području kibersigurnosti? Npr. utvrđivanje općih ciljeva, opsega i/ili načela planova za nepredvidive situacije...	1	Imate li doktrinu / nacionalnu strategiju koja uključuje kibersigurnost kao čimbenik krize (tj. nacrt, politiku itd.)?	1	Imate li plan upravljanja kiberkrizom na nacionalnoj razini?	1	Jeste li zadovoljni brojem ili postotkom ključnih sektora uključenih u nacionalni plan za nepredvidive situacije u području kibersigurnosti?	1	Imate li uspostavljen postupak stjecanja iskustava nakon vježbi u području kibersigurnosti ili stvarnih kriza na nacionalnoj razini?	1
	2	Je li općenito razumljivo da kiberincidenti predstavljaju krizni čimbenik koji bi mogao ugroziti nacionalnu sigurnost?	0	Imate li centar za prikupljanje informacija i informiranje donositelja odluka, tj. bilo kakve metode, platforme ili lokacije kako bi se osiguralo da svi subjekti uključeni u odgovor na krizu mogu pristupiti istim informacijama o kiberkrizi u stvarnom vremenu?	1	Imate li postupke specifične za kiberkrizu na nacionalnoj razini?	1	Organizirate li dovoljno često aktivnosti (tj. vježbe) povezane s nacionalnim planom za nepredvidive situacije u području kibersigurnosti?	1	Imate li postupak za redovito ispitivanje nacionalnog plana?	1
	3	Jesu li provedene studije (tehničke, operativne, političke) u vezi s planovima za nepredvidive situacije u području kibersigurnosti?	0	Jesu li relevantni resursi uključeni u nadzor razvoja i provedbe nacionalnih planova za nepredvidive situacije u području kibersigurnosti?	1	Imate li komunikacijski tim posebno osposobljen za odgovor na kiberkrize i informiranje javnosti?	1	Imate li dovoljno ljudi posvećenih planiranju u kriznim situacijama, razmatranju stečenih iskustava i provedbi promjena?	1	Imate li odgovarajuće alate i platforme za informiranost o stanju?	1
	4	-		Imate li metodologiju za procjenu kiberprijetnji na nacionalnoj razini koja obuhvaća postupke za procjenu učinka?	0	Uključujete li sve relevantne nacionalne dionike (nacionalnu sigurnost, obranu, civilnu zaštitu, tijela za izvršavanje zakonodavstva, ministarstva, nadležna tijela itd.)?	1	Imate li dovoljno ljudi osposobljenih za odgovor na kiberkrize na nacionalnoj razini?	1	Primjenjujete li poseban model zrelosti za praćenje i poboljšanje plana za nepredvidive situacije u području kibersigurnosti?	0

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	5	-		-		Imate li odgovarajuće objekte za upravljanje krizom i sobe za krizne situacije?	1	-		Imate li resurse specijalizirane za predviđanje prijetnji ili rad na budućoj kibersigurnosti radi rješavanja budućih kriza ili budućih izazova?	0
	6	-		-		Surađujete li s međunarodnim dionicima u EU-u ako je to potrebno?	0	-		-	
	7	-		-		Surađujete li s međunarodnim dionicima u zemljama izvan EU-a ako je to potrebno?	0	-		-	
2 – Utvrđivanje osnovnih sigurnosnih mjera	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li proveli studiju za utvrđivanje zahtjeva i nedostataka za **javne** organizacije na temelju međunarodno priznatih normi? Npr. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Jesu li sigurnosne mjere donesene u skladu s međunarodnim/nacionalnim normama?	1	Jesu li osnovne sigurnosne mjere obvezne?	1	Postoji li postupak za često ažuriranje osnovnih sigurnosnih mjera?	1	Imate li postupak za jačanje IKT-a kada se incidenti ne rješavaju s pomoću mjera?	1
	2	Jeste li proveli studiju za utvrđivanje zahtjeva i nedostataka za **privatne** organizacije na temelju međunarodno priznatih normi? Npr. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Provode li se savjetovanja s privatnim sektorom i drugim dionicima pri definiranju osnovnih sigurnosnih mjera?	1	Provodite li horizontalne sigurnosne mjere u ključnim sektorima?	1	Postoji li mehanizam praćenja za ispitivanje primjene osnovnih sigurnosnih mjera?	1	Ocjenjujete li relevantnost novih normi koje su uspostavljene kao odgovor na najnovija kretanja u okruženju prijetnji?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	3	-		-		Provodite li sigurnosne sektorske mjere u ključnim sektorima?	1	Postoji li nacionalno tijelo koje provjerava provode li se osnovne sigurnosne mjere?	1	Imate li ili promičete li nacionalni postupak koordiniranog otkrivanja ranjivosti (CVD)?	1
	4	-				Jesu li osnovne sigurnosne mjere u skladu s relevantnim programima certifikacije?	1	Imate li uspostavljen postupak za identifikaciju organizacija koje ne ispunjavaju zahtjeve u određenom vremenskom razdoblju?	1	-	
	5	-		-		Postoji li postupak samoprocjene rizika za osnovne sigurnosne mjere?	1	Postoji li postupak revizije kako bi se osigurala pravilna primjena sigurnosnih mjera?	1	-	
2 – Utvrđivanje osnovnih sigurnosnih mjera	6	-		-		Preispitujete li obvezne osnovne sigurnosne mjere u postupku javne nabave državnih tijela?	0	Definirate li ili aktivno potičete donošenje sigurnih normi za razvoj ključnih proizvoda informacijske/operativne tehnologije (medicinska oprema, povezana i autonomna vozila, profesionalni radio, oprema za tešku industriju...)?	0	-	
3 – Siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li proveli studije ili analize nedostataka kako biste utvrdili potrebe za osiguravanjem digitalnih javnih usluga za građane i poduzeća?	1	Provodite li analize rizika kako biste utvrdili profil rizičnosti imovine ili usluga prije nego što ih prenesete u oblak ili pokrenete projekte digitalne transformacije?	1	Promičete li metodologije integrirane privatnosti u svim projektima e-vlade?	1	Prikupljate li pokazatelje o kiberincidentima koji uključuju kršenje digitalnih javnih usluga?	1	Sudjelujete li u europskim radnim skupinama radi održavanja normi ili osmišljavanja novih zahtjeva za elektroničke usluge povjerenja (e-potpisi, e-pečati, usluge e-registrirane dostave, vremenski žig, autentifikacija mrežnih mjesta)? Npr. ETSI/CENELEC, ISO, IETF, NIST, ITU...	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
3 – Siguran digitalni identitet i izgradnja povjerenja u digitalne javne usluge	2	-		Imate li strategiju za izgradnju ili promicanje sigurnih nacionalnih sustava elektroničke identifikacije za građane i poduzeća?	1	Uključujete li privatne dionike u osmišljavanje i pružanje sigurnih digitalnih javnih usluga?	1	Jeste li proveli uzajamno priznavanje sredstava e-identifikacije s drugim državama članicama?	1	Sudjelujete li aktivno u istorazinskim ocjenama u okviru obavješćivanja Europske komisije o sustavima elektroničke identifikacije?	1
	3	-		Imate li strategiju za izgradnju ili promicanje sigurnih nacionalnih elektroničkih usluga povjerenja (e-potpisi, e-pečati, usluge e-registrirane dostave, vremenski žig, autentifikacija mrežnih mjesta) za građane i poduzeća?	1	Primjenjujete li minimalne sigurnosne standarde za sve digitalne javne usluge?	1	-		-	
	4	-		Imate li strategiju o oblaku vlade (strategija računalstva u oblaku usmjerena na vladu i državna tijela kao što su ministarstva, državne agencije i javna uprava...) u kojoj se uzimaju u obzir posljedice za sigurnost?	0	Jesu li sustavi elektroničke identifikacije dostupni građanima i poduzećima sa znatnom ili visokom razinom sigurnosti kako je definirano u Prilogu Uredbi (EU) br. 910/2014 o elektroničkoj identifikaciji?	1	-		-	
	5	-		-		Imate li digitalne javne usluge za koje su potrebni sustavi elektroničke identifikacije sa znatnom ili visokom razinom sigurnosti kako je definirano u Prilogu Uredbi (EU) br. 910/2014 o elektroničkoj identifikaciji?	1	-		-	
	6	-		-		Imate li pružatelje usluga povjerenja za građane i poduzeća (e-potpisi, e-pečati, usluge e-registrirane dostave, vremenski žig, autentifikacija mrežnih mjesta)?	1	-		-	
	7	-		-		Potičete li donošenje osnovnih sigurnosnih mjera za sve modele uvođenja oblaka (npr. privatne, javne, hibridne, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Klaster br. 2: Izgradnja kapaciteta i podizanje svijesti

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
4 – Uspostava sposobnosti odgovora na incidente	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Upravljate li neformalnim kapacitetima za odgovor na incidente unutar ili između javnog i privatnog sektora?	1	Imate li najmanje jedan službeni nacionalni tim za odgovor na računalne sigurnosne incidente?	1	Imate li kapacitete za odgovor na incidente za sektore navedene u Prilogu II. Direktivi NIS?	1	Jeste li definirali i promicali standardizirane prakse za postupke odgovora na incidente i sustave klasifikacije incidenata?	1	Imate li mehanizme za rano otkrivanje, identifikaciju, suzbijanje i ublažavanje ranjivosti nultog dana te odgovor na njih?	1
	2	-		Ima li vaš nacionalni tim za odgovor na računalne sigurnosne incidente jasno definirano područje intervencije? Npr. ovisno o ciljanom sektoru, vrstama incidenata, učincima.	1	Postoji li u vašoj zemlji mehanizam za suradnju timova za odgovor na računalne sigurnosne incidente u cilju odgovora na incidente?	1	Ocjenjujete li svoju sposobnost odgovora na incidente kako biste osigurali da imate odgovarajuće resurse i vještine za obavljanje zadaća navedenih u točki 2. Priloga I. Direktivi NIS?	1	-	
	3	-		Imaju li vaš nacionalni timovi za odgovor na računalne sigurnosne incidente jasno definirane odnose s drugim nacionalnim dionicima u pogledu nacionalne prakse u okruženju kibersigurnosti i prakse odgovora na incidente (npr. agencija za izvršavanje zakonodavstva, vojska, pružatelji internetskih usluga, nacionalni koordinacijski centri)?	0	Imaju li vaš nacionalni timovi za odgovor na računalne sigurnosne incidente sposobnost odgovora na incidente u skladu s Prilogom I. Direktivi NIS, tj. dostupnost, fizičku sigurnost, kontinuitet poslovanja, međunarodnu suradnju, praćenje incidenata, kapacitet ranog upozoravanja i uzbunjivanja, odgovor na incidente, analizu rizika i informiranost o stanju, suradnju s privatnim sektorom, standardne prakse...	1	-		-	
	4	-				Postoji li mehanizam suradnje s drugim susjednim zemljama u pogledu incidenata?	1	-		-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
4 – Uspostava sposobnosti odgovora na incidente	5	-		-		Jeste li formalno definirali jasne politike i postupke za rješavanje incidenata?	1	-		-	
	6	-		-		Sudjeluju li vaši nacionalni timovi za odgovor na računalne sigurnosne incidente u vježbama u području kibersigurnosti na nacionalnoj i međunarodnoj razini?	1	-		-	
	7	-		-		Jesu li vaši nacionalni timovi za odgovor na računalne sigurnosne incidente povezani s FIRST-om (Forumom timova za odgovor na incidente i sigurnosnim timovima)?	0	-		-	
5 – Podizanje svijesti korisnika	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jesu li vlada, privatni sektor i opći korisnici svjesni potrebe razvoja svijesti u pitanjima kibersigurnosti i privatnosti?	1	Jeste li utvrdili posebnu ciljnu publiku za informiranje korisnika? Npr. opći korisnici, mladi, poslovni korisnici (koji se mogu dodatno raščlaniti: MSP-ovi, operatori ključnih usluga, pružatelji digitalnih usluga itd.).	1	Jeste li izradili komunikacijske planove/strategiju za kampanje?	1	Izrađujete li parametre za procjenu vaše kampanje tijekom faze planiranja?	1	Imate li uspostavljene mehanizme kojima se osigurava stalna relevantnost kampanja za podizanje svijesti u pogledu tehnološkog napretka, promjena u području prijetnji, pravnih propisa i direktiva o nacionalnoj sigurnosti?	1
	2	Provode li javne agencije u okviru svoje organizacije kampanje za podizanje svijesti o kibersigurnosti na *ad hoc* osnovi, npr. nakon kiberincidenta?	0	Izrađujete li projektni plan za podizanje svijesti o pitanjima informacijske sigurnosti i privatnosti?	1	Imate li postupak izrade sadržaja na državnoj razini?	1	Ocjenjujete li svoje kampanje nakon provedbe?	1	Provodite li periodičnu procjenu ili studiju za mjerenje promjene stavova ili ponašanja u pogledu kibersigurnosti i pitanja privatnosti u privatnom i javnom sektoru?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
5 – Podizanje svijesti korisnika	3	Provode li državna tijela u javnosti kampanje za podizanje svijesti o kibersigurnosti na *ad hoc* osnovi, npr. nakon incidenta povezanog s kibersigurnošću?	0	Imate li resurse koji su dostupni i lako prepoznatljivi (npr. jedinstveni internetski portal, kompleti alata za podizanje svijesti) i namijenjeni svim korisnicima koji se žele obrazovati o informacijama o kibersigurnosti i pitanjima privatnosti?	1	Imate li mehanizme za utvrđivanje ciljnih područja za podizanje svijesti (tj. prijetnje koje je utvrdila ENISA, stanje na nacionalnoj i međunarodnoj razini, povratne informacije nacionalnih centara za kiberkriminalitet itd.)?	1	Imate li uspostavljene mehanizme za utvrđivanje najrelevantnijih medijskih ili komunikacijskih kanala ovisno o ciljanoj publici kako bi se maksimalno povećao doseg i angažman? Npr. različite vrste digitalnih medija, brošure, e-poruke, nastavni materijali, plakati na frekventnim područjima, televizija, radio...	1	Savjetujete li se sa stručnjacima za ponašanje kako biste svoju kampanju prilagodili ciljanoj publici?	1
	4	-		-		Povezujete li dionike sa stručnjacima i timovima za komunikaciju radi izrade sadržaja?	1			-	
	5	-		-		Uključujete li privatni sektor u svoje napore u pogledu podizanja svijesti kako biste promicali i prenosili poruke široj publici?	1	-		-	
	6	-		-		Pripremate li posebne inicijative za podizanje svijesti za rukovoditelje u javnom, privatnom, akademskom sektoru ili sektoru civilnog društva?	1	-		-	
	7	-		-		Sudjelujete li u kampanjama u okviru europskog mjeseca kibersigurnosti koji organizira ENISA?	0	-		-	
6 – Organizacija vježbi u području kibersigurnosti	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
6 – Organizacija vježbi u području kibersigurnosti	1	Provodite li vježbe simulacije krize u drugim sektorima (osim kibersigurnosti) na nacionalnoj ili paneuropskoj razini?	1	Imate li program vježbi u području kibersigurnosti na nacionalnoj razini?	1	Uključujete li sva povezana tijela javne uprave? (čak i ako je scenarij specifičan za određeni sektor)	1	Sastavljate li izvješća nakon aktivnosti / izvješća o procjeni?	1	Imate li kapacitet za analizu stečenih iskustava u pogledu kibersigurnosti (procesi izvješćivanja, analiza, ublažavanje)?	1
	2	Imate li resurse dodijeljene za osmišljavanje i planiranje vježbe upravljanja krizama?	1	Provodite li ili dajete prednost vježbama upravljanja kiberkrizom u okviru ključnih društvenih funkcija i ključne infrastrukture?	1	Uključujete li privatni sektor u planiranje i provedbu vježbi?	1	Ispitujete li planove i postupke na nacionalnoj razini?	1	Imate li uspostavljen postupak stjecanja iskustava?	1
	3	-		Jeste li utvrdili koordinacijsko tijelo za nadgledanje izrade i planiranja vježbi u području kibersigurnosti (javna agencija, konzultant...)?	0	Organizirate li vježbe za pojedine sektore na nacionalnoj ili međunarodnoj razini?	1	Sudjelujete li u vježbama u području kibersigurnosti na paneuropskoj razini?	1	Prilagođavate li scenarije vježbe ovisno o najnovijem razvoju događaja (tehnološki napredak, globalni sukobi, prijetnje...)?	1
	4	-		-		Organizirate li vježbe u svim ključnim sektorima navedenima u Prilogu II. Direktivi NIS?	1	-		Usklađujete li svoje postupke upravljanja krizama s drugim državama članicama radi osiguravanja djelotvornog paneuropskog upravljanja krizama?	1
	5	-		-		Organizirate li međusektorske vježbe ili vježbe unutar sektora u području kibersigurnosti?	1	-		Imate li mehanizam za brzu prilagodbu strategije, planova i postupaka na temelju iskustava stečenih tijekom vježbi?	0
	6	-		-		Organizirate li vježbe u području kibersigurnosti specifične za različite razine (tehnička i operativna razina, razina postupka, razina odlučivanja, politička razina...)?	0	-		-	
7 – Jačanje programa osposobljavanja i izobrazbe	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	1	Razmatrate li izradu programa osposobljavanja i izobrazbe u području kibersigurnosti?	1	Uspostavljate li tečajeve u području kibersigurnosti?	1	Ima li vaša zemlja kulturu kibersigurnosti u ranoj fazi obrazovanja učenika? Na primjer, podržavate li temu kibersigurnosti u srednjim školama?	1	Potičete li osoblje u privatnom i javnom sektoru na akreditaciju ili certifikaciju?	1	Imate li uspostavljene mehanizme kojima se osigurava stalna relevantnost programa osposobljavanja i izobrazbe u pogledu postojećeg i novog tehnološkog razvoja, promjena u području prijetnji, pravnih propisa i direktiva o nacionalnoj sigurnosti?	1
	2	-		Nude li sveučilišta u vašoj zemlji doktorate u području kibersigurnosti kao neovisnu disciplinu, a ne kao predmet u okviru računalstva?	1	Imate li nacionalne istraživačke laboratorije i obrazovne ustanove specijalizirane za kibersigurnost?	1	Je li vaša zemlja razvila programe osposobljavanja ili mentorstva u području kibersigurnosti kako bi pružila potporu nacionalnim novoosnovanim poduzećima i MSP-ovima?	1	Uspostavljate li akademske centre izvrsnosti u području kibersigurnosti koji će djelovati kao centri za istraživanje i obrazovanje?	1
	3	-		Planirate li osposobiti nastavnike, neovisno o njihovu području, u pitanjima informacijske sigurnosti i privatnosti ? Npr. sigurnosti na internetu, zaštiti osobnih podataka, kiberzlostavljanju.	1	Potičete li ili financirate specijalizirane tečajeve i planove osposobljavanja u području kibersigurnosti za zaposlenike zavoda za zapošljavanje u državama članicama?	1	Jeste li aktivni u promicanju uvrštavanja kolegija u vezi s informacijskom sigurnošću u visoko obrazovanje, ne samo za studente u području informatike, nego i u svim ostalim područjima? Npr. kolegiji prilagođeni potrebama te profesije.	1	Sudjeluju li akademske ustanove u raspravama u području obrazovanja i istraživanja u pogledu kibersigurnosti na međunarodnoj razini?	0
	4	-		-		Imate li tečajeve za kibersigurnost ili specijalizirani program za Europski kvalifikacijski okvir razine od 5 do 8?	1	Procjenjujete li redovito nedostatak vještina (manjak radnika u području kibersigurnosti) u pogledu informacijske sigurnosti?	1	-	
	5	-		-		Potičete li ili podržavate inicijative za uključivanje predmeta o sigurnosti na internetu u osnovnoškolsko i srednjoškolsko obrazovanje?	1	Potičete li umrežavanje i razmjenu informacija među akademskim ustanovama na nacionalnoj i međunarodnoj razini?	1		

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
7 - Jačanje programa osposobljavanja i izobrazbe	6	-		-		Financirate li ili nudite besplatno osnovno osposobljavanje u području kibersigurnosti za građane?	0	Uključujete li privatni sektor u bilo kojem obliku u obrazovne inicijative u području kibersigurnosti? Npr. osmišljavanje i provedba tečajeva, stažiranje, pripravništvo...	1	-	
	7	-		-		Organizirate li godišnje manifestacije u području informacijske sigurnosti (npr. hakerski natječaji ili hakatoni)?	0	Provodite li mehanizme financiranja kako biste potaknuli stjecanje diploma u području kibersigurnosti? Npr. stipendije, zajamčeno naukovanje/pripravništvo, zajamčeni poslovi u određenoj industriji ili uloge u javnom sektoru.	0	-	
8 – Poticanje istraživanja i razvoja	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li proveli studije ili analize za utvrđivanje prioriteta istraživanja i razvoja u području kibersigurnosti?	1	Imate li postupak utvrđivanja prioriteta u području istraživanja i razvoja (npr. nove teme za odvraćanje i zaštitu od kibernapada, njihovo otkrivanje i prilagodbu novim vrstama kibernapada)?	1	Postoji li plan za povezivanje inicijativa u vezi s istraživanjem i razvojem s realnim gospodarstvom?	1	Jesu li inicijative u vezi s istraživanjem i razvojem u području kibersigurnosti u skladu s relevantnim strateškim ciljevima, npr. jedinstveno digitalno tržište, Obzor 2020., Digitalna Europa, strategija EU-a za kibersigurnost?	1	Surađujete li na nacionalnoj razini s nekim međunarodnim inicijativama u vezi s istraživanjem i razvojem u području kibersigurnosti?	1
	2	-		Je li privatni sektor uključen u utvrđivanje prioriteta istraživanja i razvoja?	1	Jesu li uspostavljeni nacionalni projekti povezani s kibersigurnošću?	1	Postoji li program procjene za inicijative u području istraživanja i razvoja?	1	Jesu li prioriteti istraživanja i razvoja usklađeni s postojećim ili budućim propisima (na nacionalnoj razini)?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
8 – Poticanje istraživanja i razvoja	3	-		Sudjeluje li akademska zajednica u utvrđivanju prioriteta istraživanja i razvoja?	1	Imate li lokalne/regionalne ekosustave novoosnovanih poduzeća i druge kanale umrežavanja (npr. tehnološke parkove, inovacijske klastere, događanja/platforme za umrežavanje) za poticanje inovacija (uključujući za novoosnovana poduzeća u području kibersigurnosti)?	1	Postoje li sporazumi o suradnji sa sveučilištima i drugim istraživačkim ustanovama?	1	Sudjelujete li u raspravama o jednoj ili više najsuvremenijih tema istraživanja i razvoja na međunarodnoj razini?	0
	4	-		Postoje li inicijative u vezi s istraživanjem i razvojem u području kibersigurnosti na nacionalnoj razini?	0	Postoje li ulaganja u programe istraživanja i razvoja u području kibersigurnosti u akademskoj zajednici i privatnom sektoru?	1	Postoji li priznato institucijsko tijelo za nadzor aktivnosti istraživanja i razvoja u području kibersigurnosti?	0	-	
	5	-		-		Imate li katedre za industrijsko istraživanje na sveučilištima kako biste povezali istraživačke teme i potrebe tržišta?	1	-		-	
	6	-		-		Imate li namjenske programe financiranja u području istraživanja i razvoja za kibersigurnost?	0	-		-	
9 – Pružanje poticaja privatnom sektoru za ulaganje u sigurnosne mjere	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Postoji li industrijska politika ili politička volja za poticanje razvoja industrije kibersigurnosti?	1	Je li privatni sektor uključen u osmišljavanje poticaja?	1	Postoje li gospodarski/regulatorni ili drugi poticaji za promicanje ulaganja u kibersigurnost?	1	Postoje li privatni subjekti koji reagiraju na poticaje ulaganjem u sigurnosne mjere ? Npr. ulagatelji specijalizirani za kibersigurnost i nespecijalizirani ulagatelji.	1	Usmjeravate li poticaje na teme kibersigurnosti ovisno o najnovijem razvoju prijetnji?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
9 – Pružanje poticaja privatnom sektoru za ulaganje u sigurnosne mjere	2	–		Jeste li utvrdili posebne teme kibersigurnosti koje treba razviti? Npr. kriptografija, privatnost, novi oblik autentifikacije, umjetna inteligencija za kibersigurnost...	0	Pružate li potporu (npr. porezni poticaji) novoosnovanim poduzećima i MSP-ovima u području kibersigurnosti?	1	Potičete li privatni sektor da se usredotoči na sigurnost najsuvremenijih tehnologija? Npr. 5G, umjetna inteligencija, internet stvari, kvantno računalstvo...	1	–	
	3	–		–		Nudite li porezne poticaje ili drugu financijsku motivaciju za ulagače iz privatnog sektora u novoosnovana poduzeća u području kibersigurnosti?	1	–		–	
	4	–		–		Olakšavate li novoosnovanim poduzećima i MSP-ovima području kibersigurnosti pristup postupku javne nabave?	0	–		–	
	5	–		–		Postoji li proračun za pružanje poticaja privatnom sektoru?	0	–		–	
10 – Poboljšanje kibersigurnosti lanca opskrbe	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li proveli studiju o sigurnosnim dobrim praksama za upravljanje lancem opskrbe koja se upotrebljava u nabavi u različitim segmentima industrije ili u javnom sektoru?	1	Provodite li kibersigurnosne procjene duž cijelog lanca opskrbe IKT usluga i proizvoda u ključnim sektorima (kako je utvrđeno u Prilogu II. Direktivi NIS (2016/1148))?	1	Upotrebljavate li program sigurnosne certifikacije za proizvode i usluge koji se temelje na IKT-u? Npr. SOG-IS MRA u Europi (Skupina viših dužnosnika za sigurnost informacijskih sustava, Sporazum o uzajamnom priznavanju), Sporazum o zajedničkim kriterijima za priznavanje (CCRA), nacionalne inicijative, sektorske inicijative...	1	Imate li uspostavljen postupak ažuriranja kibersigurnosnih procjena lanca opskrbe IKT usluga i proizvoda u ključnim sektorima (kako je utvrđeno u Prilogu II. Direktivi NIS (2016/1148))?	1	Imate li testove za otkrivanje u okviru ključnih elemenata lanca opskrbe kako bi se otkrili rani znakovi ugroze? Npr. sigurnosne kontrole na razini pružatelja internetskih usluga, sigurnosni testovi u glavnim infrastrukturnim komponentama...	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
10 – Poboljšanje kibersigurnosti lanca opskrbe	2	-		Primjenjujete li norme u politikama javne nabave javnih uprava kako bi se osiguralo da pružatelji IKT proizvoda ili usluga ispunjavaju osnovne zahtjeve informacijske sigurnosti? Npr. ISO/IEC 27001 i 27002, ISO/IEC 27036...	1	Promičete li aktivno sigurnost i privatnost osmišljavanjem najboljih praksi u razvoju IKT proizvoda i usluga? Npr. životni ciklus sigurnog razvoja softvera, životni ciklus interneta stvari.	1	Imate li postupak za utvrđivanje slabih karika u pogledu kibersigurnosti u lancu opskrbe u ključnim sektorima (kako je utvrđeno u Prilogu II. Direktivi NIS (2016/1148))?	1	-	
	3	-		-		Izrađujete li i stavljate na raspolaganje centralizirane kataloge s proširenim informacijama o postojećim normama informacijske sigurnosti i privatnosti koje MSP-ovi mogu nadograditi i primjenjivati?	1	Imate li mehanizme kojima se osigurava da su proizvodi i usluge IKT-a koji su ključni za operatore ključnih usluga kiberotporni (tj. mogu održati dostupnost i sigurnost u slučaju kiberincidenata)? Npr. testiranjem, redovitim procjenama, otkrivanjem kompromitiranih elemenata...	1	-	
	4	-				Sudjelujete li aktivno u oblikovanju okvira EU-a za certifikaciju digitalnih proizvoda, usluga i procesa IKT-a kako je utvrđeno u aktu EU-a o kibersigurnosti (Uredba (EU) 2019/881)? Npr. sudjelovanje u Europskoj skupini za kibersigurnosnu certifikaciju (ECCG), promicanje tehničkih normi i postupaka za sigurnost proizvoda/usluga IKT-a	0	Promičete li razvoj programa certifikacije usmjerenih na MSP-ove kako bi se poboljšalo usvajanje normi u području informacijske sigurnosti i privatnosti?	0	-	
	5	-		-		Pružate li MSP-ovima bilo kakve poticaje za usvajanje normi u području sigurnosti i privatnosti?	0	Imate li neke odredbe kojima se velika poduzeća potiču na povećanje kibersigurnosti malih poduzeća u svojim lancima opskrbe? Npr. centar za kibersigurnost, kampanje za osposobljavanje i podizanje svijesti...	0	-	
	6	-		-		Potičete li prodavače softvera da podrže MSP-ove osiguravanjem sigurnih zadanih konfiguracija u proizvodima namijenjenima malim organizacijama?	0	-		-	

4.1.3 Klaster br. 3: Pravna i regulatorna pitanja

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
11 – Zaštita ključne informatičke infrastrukture, operatora ključnih usluga i pružatelja digitalnih usluga	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Postoji li opće shvaćanje da operatori ključne informatičke infrastrukture doprinose nacionalnoj sigurnosti?	1	Imate li metodologiju za utvrđivanje ključnih usluga?	1	Jeste li proveli Direktivu NIS (2016/1148)?	1	Imate li postupak za ažuriranje registra rizika?	1	Izrađujete li i ažurirate izvješća o prijetnjama?	1
	2	-		Imate li metodologiju za utvrđivanje ključne informatičke infrastrukture?	1	Jeste li proveli Direktivu o europskoj građanskoj inicijativi (2008/114) o utvrđivanju i označivanju europske ključne infrastrukture i procjeni potrebe poboljšanja njezine zaštite?	1	Imate li druge mehanizme za mjerenje primjerenosti tehničkih i organizacijskih mjera koje provodi operator ključnih usluga za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi? Npr. redovite revizije kibersigurnosti, nacionalni okvir za provedbu standardnih mjera, tehnički alati koje osigurava vlada, kao što su testovi za otkrivanje ili pregled konfiguracije specifične za sustav...	1	Ovisno o najnovijim kretanjima u području prijetnji, možete li uključiti novi sektor u svoj akcijski plan za zaštitu ključne informatičke infrastrukture?	1
	3	-		Imate li metodologiju za utvrđivanje operatora ključnih usluga?	1	Imate li nacionalni registar za utvrđene operatore ključnih usluga po ključnom sektoru?	1	Preispitujete li i ažurirate popis utvrđenih operatora ključnih usluga najmanje svake dvije godine?	1	Ovisno o najnovijim kretanjima u području prijetnji, možete li prilagoditi nove zahtjeve u svojem akcijskom planu za zaštitu ključne informatičke infrastrukture?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
11 – Zaštita ključne informatičke infrastrukture, operatora ključnih usluga i pružatelja digitalnih usluga	4	-		Imate li metodologiju za utvrđivanje pružatelja digitalnih usluga?	1	Imate li nacionalni registar za utvrđene pružatelje digitalnih usluga?	1	Imate li druge mehanizme za mjerenje primjerenosti tehničkih i organizacijskih mjera koje provode pružatelji digitalnih usluga za upravljanje rizicima za sigurnost mrežnih i informacijskih sustava? Npr. redovite revizije kibersigurnosti, nacionalni okvir za provedbu standardnih mjera, tehnički alati koje osigurava vlada, kao što su testovi za otkrivanje ili pregled konfiguracije specifične za sustav.	1	-	
	5	-		Imate li jedno ili više nacionalnih tijela koja provode nadzor nad zaštitom ključne informatičke infrastrukture i sigurnosti mrežnih i informacijskih sustava, npr. u skladu s Direktivom NIS (2016/1148)?	1	Imate li nacionalni registar rizika za utvrđene ili poznate rizike?	1	Preispitujete li i ažurirate popis utvrđenih pružatelja digitalnih usluga barem svake dvije godine?	1	-	
	6	-		Razvijate li sektorske planove zaštite, npr. uključujući osnovne mjere kibersigurnosti (obvezne mjere ili smjernice)?	0	Imate li metodologiju za mapiranje ovisnosti o ključnoj informatičkoj infrastrukturi?	1	Koristite li program sigurnosnog certificiranja (nacionalni ili međunarodni) kako biste pomogli operatorima ključnih usluga i pružateljima digitalnih usluga u prepoznavanju sigurnih IKT proizvoda? Npr. SOG-IS MRA u Europi, nacionalne inicijative...	1	-	
	7	-		-		Primjenjujete li prakse upravljanja rizikom kako biste utvrdili i kvantificirali rizike povezane s ključnom informatičkom infrastrukturom na nacionalnoj razini i upravljali tim rizicima?	1	Koristite li program sigurnosne certifikacije ili kvalifikacijski postupak za ocjenjivanje pružatelja usluga koji rade s operatorom ključnih usluga? Npr. pružatelji usluga u području otkrivanja incidenata, odgovora na incidente, revizije u području sigurnosti, usluga u oblaku, pametnih kartica...	1	-	
	8	-		-		Sudjelujete li u postupku savjetovanja radi utvrđivanja prekograničnih ovisnosti?	1	Imate li uspostavljene mehanizme za mjerenje razine usklađenosti operatora ključnih usluga i pružatelja digitalnih usluga u pogledu osnovnih mjera kibersigurnosti?	0	-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
11 – Zaštita ključne informatičke infrastrukture, operatora ključnih usluga i pružatelja digitalnih usluga	9					Imate li jedinstvenu točku za kontakt nadležnu za koordinaciju pitanja povezanih sa sigurnošću mrežnih i informacijskih sustava na nacionalnoj razini i prekograničnu suradnju na razini Unije?	1	Imate li uspostavljene odredbe kako biste osigurali kontinuitet usluga koje se pružaju u okviru ključne informatičke infrastrukture? Npr. predviđanje krize, postupci za ponovnu izgradnju ključnih informacijskih sustava, kontinuitet poslovanja bez informacijske tehnologije, izrada sigurnosne kopije s pomoću postupka *air gap*...	0		
	10					Definirate li osnovne mjere kibersigurnosti (obvezne mjere ili smjernice) za pružatelje digitalnih usluga i sve sektore utvrđene u Prilogu II. Direktivi NIS (2016/1148)?	1				
	11	-		-		Osiguravate li alate ili metodologije za otkrivanje kiberincidenata?	1	-		-	
12 – Borba protiv kiberkriminaliteta	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	1	Jeste li proveli studiju kako biste utvrdili zahtjeve tijela za provedbu zakonodavstva (pravna osnova, resursi, vještine...) radi djelotvornog rješavanja pitanja kiberkriminaliteta?	1	Je li vaš nacionalni pravni okvir u potpunosti usklađen s relevantnim pravnim okvirom EU-a, uključujući Direktivu 2013/40/EU o napadima na informacijske sustave? Npr. nezakonit pristup informacijskim sustavima, nezakonito ometanje sustava, nezakonito ometanje podataka, nezakonito presretanje, alati koji se upotrebljavaju za počinjenje kaznenih djela...	1	Imate li odjele posvećene kiberkriminalitetu u uredima tužiteljstva?	1	Prikupljate li statističke podatke u skladu s odredbama članka 14. stavka 1. Direktive 2013/40/EU (Direktiva o napadima na informacijske sustave)?	1	Imate li međuinstitucijsku obuku ili radionice za osposobljavanje za agencije za izvršavanje zakonodavstva, sudce, tužitelje i nacionalne/državne timove za odgovor na računalne sigurnosne incidente na nacionalnoj ili multilateralnoj razini?	1
	2	Jeste li proveli studiju kako biste utvrdili zahtjeve tužitelja i sudaca (pravna osnova, resursi, vještine...) za djelotvornu borbu protiv kiberkriminaliteta?	1	Imate li pravne odredbe koje se odnose na krađu identiteta na internetu i krađu osobnih podataka?	1	Raspolažete li namjenskim proračunom namijenjenim jedinicama za kiberkriminalitet?	1	Prikupljate li odvojene statističke podatke o kiberkriminalitetu? Npr. operativne statističke podatke, statističke podatke o trendovima kiberkriminaliteta, statističke podatke o prihodima od kiberkriminaliteta i prouzročenoj šteti...	1	Sudjelujete li u koordiniranim mjerama na međunarodnoj razini kako bi se prekinule kriminalne aktivnosti? Npr. infiltracija u zločinačke forume za hakiranje, organizirane skupine za kiberkriminalitet, tržište mračne mreže, uklanjanje botnetova...	1
	3	Je li vaša zemlja potpisala Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu?	1	Imate li pravne odredbe koje se odnose na povrede intelektualnog vlasništva i autorskih prava na internetu?	1	Jeste li uspostavili središnje tijelo/subjekt za koordinaciju aktivnosti u području borbe protiv kiberkriminaliteta?	1	Ocjenjujete li prikladnost osposobljavanja koje se pruža tijelima za izvršavanje zakonodavstva, pravosudnim djelatnicima i nacionalnim timova za odgovor na računalne sigurnosne incidente za borbu protiv kiberkriminaliteta?	1	Postoji li jasna podjela dužnosti među timovima za odgovor na računalne sigurnosne incidente, agencijama za izvršavanje zakonodavstva i pravosudnim tijelima (tužitelji i sudci) kada surađuju u borbi protiv kiberkriminaliteta?	1
	4			Imate li pravne odredbe o uznemiravanju na internetu ili kiberzlostavljanju?	1	Jeste li uspostavili mehanizme suradnje među relevantnim nacionalnim institucijama uključenima u borbu protiv kiberkriminaliteta, uključujući nacionalne timove za odgovor na računalne sigurnosne incidente za izvršavanje zakonodavstva?	1	Provodite li redovite procjene kako biste osigurali da imate dovoljno resursa (ljudskih i proračunskih resursa te alata) namijenjenih jedinicama za kiberkriminalitet u okviru agencija za izvršavanje zakonodavstva?	1	Olakšava li vaš regulatorni okvir suradnju timova za odgovor na računalne sigurnosne incidente / agencija za izvršavanje zakonodavstva i pravosuđa (tužitelji i sudci)?	1

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
12 – Borba protiv kiberkriminaliteta	5			Imate li pravne odredbe o računalnim prijevarama, npr. usklađenost s odredbama Budimpeštanske konvencije Vijeća Europe o kibernetičkom kriminalu?	1	Surađujete li i dijelite li informacije s drugim državama članicama u području borbe protiv kiberkriminaliteta?	1	Provodite li redovite procjene kako biste osigurali da imate dovoljno resursa (ljudskih i proračunskih resursa te alata) namijenjenih jedinicama za kiberkriminalitet u okviru tijela za kazneni progon?	1	Sudjelujete li u izgradnji i održavanju normiranih alata i metodologija, obrazaca i postupaka koji će se dijeliti s dionicima iz EU-a (agencijama za izvršavanje zakonodavstva, timovima za odgovor na računalne sigurnosne incidente, ENISA-om, Europskim centrom za kiberkriminalitet u okviru Europola...)?	1
	6	-		Imate li pravne odredbe o zaštiti djece na internetu? Npr. usklađenost s odredbama Direktive 2011/93/EU i Budimpeštanskom konvencijom Vijeća Europe o kibernetičkom kriminalu...	1	Surađujete li i dijelite li informacije s agencijama EU-a (npr. Europskim centrom za kiberkriminalitet u okviru Europola, Eurojustom, ENISA-om) u području borbe protiv kiberkriminaliteta?	1	Imate li posebne sudove ili specijalizirane sudce za rješavanje predmeta povezanih s kiberkriminalitetom?	1	Imate li napredne mehanizme za odvraćanje pojedinaca od privlačenja ili uključivanja u kiberkriminalitet?	0
	7	-		Jeste li utvrdili operativnu nacionalnu točku za kontakt za razmjenu informacija i odgovaranje na hitne zahtjeve za informacije iz drugih država članica u vezi s kaznenim djelima utvrđenima u Direktivi 2013/40/EU (Direktiva o napadima na informacijske sustave)?	1	Imate li odgovarajuće alate za rješavanje problema kiberkriminaliteta? Npr. taksonomija i klasifikacija kiberkriminaliteta, alati za prikupljanje elektroničkih dokaza, alati za računalnu forenziku, pouzdane platforme za razmjenu...	1	Imate li mogućnosti pružanja potpore i pomoći žrtvama kiberkriminaliteta (opći korisnici, MSP-ovi, velika poduzeća)?	1	Upotrebljava li vaša država Plan EU-a i/ili Protokol EU-a za odgovor na hitne situacije (EU LE ERP) za djelotvoran odgovor na kiberincidente velikih razmjera?	0
	8			Ima li vaša agencija za izvršavanje zakonodavstva poseban odjel za kiberkriminalitet?	1	Imate li uspostavljene operativne postupke za postupanje s e-dokazima?	1	Jeste li uspostavili međuinstitucijski okvir i mehanizme suradnje među svim relevantnim dionicima (npr. agencijom za izvršavanje zakonodavstva, nacionalnim timovima za odgovor na računalne sigurnosne incidente, pravosudnim zajednicama), uključujući privatni sektor (npr. operatori ključnih usluga, pružateljima usluga) kako bi se odgovorilo na kibernapade?	1	-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
12 – Borba protiv kiberkriminaliteta	9			Jeste li imenovali točku za kontakt dežurnu 24 sata dnevno sedam dana u tjednu u skladu s člankom 35. Budimpeštanske konvencije?	1	Sudjeluje li vaša zemlja u mogućnostima osposobljavanja koje nude i/ili podržavaju agencije EU-a (npr. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Olakšava li vaš regulatorni okvir suradnju nacionalnih timova za odgovor na računalne sigurnosne incidente i tijela za izvršavanje zakonodavstva?	1	-	
	10	-		Jeste li odredili operativnu nacionalnu točku za kontakt koja će biti dežurna 24 sata dnevno sedam dana u tjednu za Protokol EU-a za odgovor na hitne situacije (EU LE ERP) kako bi se odgovorilo na velike kibernapade?	1	Razmatra li vaša zemlja donošenje 2. dodatnog protokola uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu?	0	Imate li uspostavljene mehanizme (npr. alate, postupke) kojima se olakšava razmjena informacija i suradnja nacionalnih timova za odgovor na računalne sigurnosne incidente i tijela za izvršavanje zakonodavstva i možda pravosuđa (tužitelji i sudci) u području borbe protiv kiberkriminaliteta?	1	-	
	11			Pružate li redovito specijalizirano osposobljavanje dionicima uključenima u borbu protiv kiberkriminaliteta (agencija za izvršavanje zakonodavstva, pravosuđe, timovi za odgovor na računalne sigurnosne incidente)? Npr., među ostalim, tečajevi osposobljavanja o evidentiranju/kaznenom progonu kaznenih djela omogućenih kibertehnologijama, osposobljavanje o prikupljanju elektroničkih dokaza i osiguravanju integriteta u cijelom digitalnom lancu nadzora i računalne forenzike.	1						
	12			Je li vaša zemlja ratificirala/potvrdila Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu?	1			-	-	-	
	13	-		Je li vaša zemlja potpisala i ratificirala Dodatni protokol (kriminalizacija rasističkih i ksenofobnih djela počinjenih putem računalnih sustava) uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu?	0	-	-	-		-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
13 – Uspostava mehanizama za izvješćivanje o incidentima	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i utvrđenim upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Imate li neformalne mehanizme za razmjenu informacija o kiberincidentima između privatnih organizacija i nacionalnih tijela?	1	Imate li program izvješćivanja o incidentima za sve sektore iz Priloga II. Direktivi NIS?	1	Imate li program obveznog izvješćivanja o incidentima koji funkcionira u praksi?	1	Imate li usklađen postupak za sektorske programe izvješćivanja o incidentima?	1	Izrađujete li godišnje izvješće o incidentima?	1
	2	-		Jeste li proveli zahtjeve za obavješćivanje za pružatelje telekomunikacijskih usluga u skladu s člankom 40. Direktive (EU) 2018/1972? Direktivom se od država članica zahtijeva da osiguraju da pružatelji javne elektroničke komunikacijske mreže ili javno dostupnih elektroničkih komunikacijskih usluga obavijeste bez nepotrebne odgode nadležno tijelo o sigurnosnom incidentu koji je znatno utjecao na rad mreža ili usluga.	1	Postoji li mehanizam koordinacije/suradnje za obveze izvješćivanja o incidentima u pogledu Opće uredbe o zaštiti podataka, Direktive NISD, članka 40. (bivši članak 13.a) i eIDAS-a?	1	Imate li program izvješćivanja o incidentima za sektore koji nisu obuhvaćeni Direktivom NIS?	1	Postoje li izvješća o kibersigurnosti ili druge vrste analiza koje je pripremio subjekt koji prima izvješća o incidentima?	1
13 – Uspostava mehanizama za izvješćivanje o incidentima	3	-		Jeste li proveli zahtjeve za prijavu za pružatelje usluga povjerenja u skladu s člankom 19. Uredbe o elektroničkoj identifikaciji (Uredba (EU) br. 910/2014)? Člankom 19. propisuje se, među ostalim, da pružatelji usluga povjerenja obavijeste nadzorno tijelo o značajnim incidentima/povredama.	1	Imate li odgovarajuće alate za osiguravanje povjerljivosti i cjelovitosti informacija koje se razmjenjuju putem različitih kanala za izvješćivanje?	1	Mjerite li djelotvornost postupaka za obavješćivanje o incidentima? Npr. pokazatelji o incidentima koji su prijavljeni putem odgovarajućih kanala, vremenski raspored izvješća o incidentima...	1	-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	4	-		Jeste li proveli zahtjeve za obavješćivanje za pružatelje digitalnih usluga u skladu s člankom 16. Direktive NIS? Člankom 16. propisuje se da pružatelji digitalnih usluga bez nepotrebne odgode trebaju obavijestiti nadležno tijelo ili tim za odgovor na računalne sigurnosne incidente o svakom incidentu koji ima znatan učinak na pružanje neke od usluga iz Priloga III. koju oni nude unutar Unije.	1	Imate li platformu/alat za olakšavanje postupka obavješćivanja?	0	Imate li zajedničku taksonomiju na nacionalnoj razini za klasifikaciju incidenata i kategorije temeljnih uzroka?	0	-	
14 – Jačanje privatnosti i zaštite podataka	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Jeste li proveli studije ili analize kako biste utvrdili područja u kojima su moguća poboljšanja radi bolje zaštite prava na privatnost građana?	1	Je li nacionalno tijelo za zaštitu podataka uključeno u područja povezana s kibersigurnošću (npr. izrada novih zakona i propisa o kibersigurnosti, definirane minimalne sigurnosne mjere)?	1	Promičete li najbolje prakse u području sigurnosnih mjera i integrirane zaštite podataka za javni i/ili privatni sektor?	1	Provodite li redovite procjene kako biste osigurali da imate dovoljno resursa (ljudskih i proračunskih resursa te alata) namijenjenih tijelu za zaštitu podataka?	1	Imate li uspostavljene mehanizme za praćenje najnovijih tehnoloških dostignuća kako bi se prilagodile relevantne smjernice i pravne odredbe/obveze?	1
	2	Jeste li razvili pravnu osnovu na nacionalnoj razini za provedbu Opće uredbe o zaštiti podataka (Uredba (EU) 2016/679)? Npr. zadržavanje ili uvođenje konkretnijih odredbi ili ograničenja pravila Uredbe.	0	-		Pokrećete li programe za podizanje svijesti i osposobljavanje u vezi s tom temom?	1	Potičete li organizacije i poduzeća da se certificiraju prema normi ISO/IEC 27701:2019 o sustavu upravljanja privatnošću informacija (PIMS)?	1	Sudjelujete li aktivno u inicijativama u području istraživanja i razvoja u pogledu tehnologija za unapređenje zaštite privatnosti (PET) odnosno promičete li takve inicijative?	0
	3	-		-		Koordinirate li postupke izvješćivanja o incidentima s tijelom za zaštitu podataka?	1	-		-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	4	-		-		Promičete li i podržavate razvoj tehničkih normi o informacijskoj sigurnosti i privatnosti? Jesu li posebno prilagođeni malim i srednjim poduzećima (MSP-ovi)?	0	-		-	
	5	-		-		Pružate li praktične i prilagodljive smjernice za potporu različitim vrstama voditelja obrade podataka pri ispunjavanju pravnih zahtjeva i obveza u pogledu privatnosti i zaštite podataka?	0	-		-	

4.1.4 Klaster br. 4: Suradnja

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
15 – Uspostava javno-privatnog partnerstva (JPP)	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						
	1	Podrazumijeva li se da se javno-privatnim partnerstvima na različite načine doprinosi podizanju razine kibersigurnosti u zemlji? Npr. dijeljenjem interesa za rast industrije kibersigurnosti, suradnjom u izgradnji relevantnog regulatornog okvira za kibersigurnost, poticanjem istraživanja i razvoja...	1	Imate li nacionalni akcijski plan za uspostavu javno-privatnih partnerstava?	1	Jeste li uspostavili nacionalna javno-privatna partnerstva?	1	Jeste li uspostavili međusektorska javno-privatna partnerstva?	1	Ovisno o najnovijim tehnološkim i regulatornim kretanjima, možete li prilagoditi ili uspostaviti javno-privatna partnerstva?	1
	2	-		Uspostavljate li pravnu ili ugovornu osnovu (posebni zakoni, ugovori o neotkrivanju podataka, intelektualno vlasništvo) za javno-privatna partnerstva?	1	Jeste li uspostavili javno-privatna partnerstva specifična za pojedine sektore?	1	Bavite li se i javno-javnom i privatno-privatnom suradnjom u okviru uspostavljenih javno-privatnih partnerstava?	1		
	3	-		–		Osiguravate li financijska sredstva za uspostavu javno-privatnih partnerstava?	1	Promičete li javno-privatna partnerstva među malim i srednjim poduzećima (MSP-ovi)?	1	-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
15 – Uspostava javno-privatnog partnerstva (JPP)	4	-		–		Vode li javne institucije općenito javno-privatna partnerstva? Točnije, jedna jedinstvena točka za kontakt iz javnog sektora koja upravlja javno-privatnim partnerstvom i koordinira ga, javna tijela unaprijed se dogovaraju o tome što žele postići, jasne smjernice javnih uprava o potrebama i ograničenjima u privatnom sektoru...	1	Mjerite li ishode javno-privatnih partnerstava?	1	-	
	5	-		–		Jeste li član ugovornog javno-privatnog partnerstva Europske organizacije za kibersigurnost (ECSO)?	0	-		-	
	6	-		-		Imate li jedno javno-privatno partnerstvo ili više njih koji se bave aktivnostima tima za odgovor na računalne sigurnosne incidente?	0	-		-	
	7					Imate li jedno javno-privatno partnerstvo ili više njih koji rade na pitanjima zaštite ključne informatičke infrastrukture?	0				
	8	-		-		Imate li jedno javno-privatno partnerstvo ili više njih koji rade na podizanju svijesti o kibersigurnosti i razvoju vještina?	0	-		-	
16 – Institucionalizacija suradnje javnih agencija	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	1	Imate li neformalne kanale za suradnju između javnih agencija?	1	Imate li nacionalni program suradnje usmjeren na kibersigurnost? Npr. savjetodavni odbori, upravljačke skupine, forumi, vijeća, kibercentri ili sastanci stručnih skupina.	1	Sudjeluju li javna tijela u programu suradnje?	1	Osiguravate li kanale suradnje u području kibersigurnosti barem među sljedećim tijelima: obavještajnim službama, nacionalnim tijelima za izvršavanje zakonodavstva, tijelima za kazneni progon, državnim subjektima, nacionalnim timovima za odgovor na nacionalne sigurnosne incidente i vojskom?	1	Pružaju li javne agencije ujednačene minimalne informacije o najnovijem razvoju situacije u pogledu prijetnji i informiranosti o stanju u području kibersigurnosti?	1
	2	-		-		Jeste li uspostavili platforme za suradnju radi razmjene informacija?	1	Mjerite li uspjeh i ograničenja različitih programa suradnje u poticanju djelotvorne suradnje?	1	-	
16 – Institucionalizacija suradnje javnih agencija	3	-		-		Jeste li definirali opseg platformi za suradnju (npr. zadaće i odgovornosti, broj spornih područja)?	1	-		-	
	4	-		-		Organizirate li godišnje sastanke?	1	-		-	
	5	-		-		Imate li mehanizme suradnje među nadležnim tijelima u geografskim regijama? Npr. mreža dopisnika za sigurnost po regiji, službenik za kibersigurnost u regionalnim gospodarskim komorama...	1	-		-	
17 – Sudjelovanje u međunarodnoj suradnji (ne samo s državama članicama EU-a)	a	Je li cilj obuhvaćen vašom postojećom nacionalnom strategijom za kibersigurnost ili ga planirate obuhvatiti sljedećim izdanjem?	1	Postoje li neslužbene prakse ili aktivnosti za ostvarivanje cilja na nekoordiniran način?	1	Imate li akcijski plan koji je formalno definiran i dokumentiran?	1	Preispitujete li svoj akcijski plan s ciljem ispitivanja njegove uspješnosti?	1	Imate li mehanizme kojima se osigurava dinamička prilagodba akcijskog plana kretanjima u pogledu okoliša?	1
	b			Jeste li definirali planirane rezultate, vodeća načela ili ključne aktivnosti svojeg akcijskog plana?	1	Imate li akcijski plan s jasnom raspodjelom resursa i upravljanjem?	1	Preispitujete li svoj akcijski plan u pogledu cilja da se osigura njegova ispravna prioritizacija i optimizacija?	1		
	c			Ako je relevantno, provodi li se vaš akcijski plan i je li već djelotvoran u ograničenom opsegu?	0						

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
17 – Sudjelovanje u međunarodnoj suradnji (ne samo s državama članicama EU-a)	1	Imate li strategiju međunarodnog angažmana?	1	Imate li sporazume o suradnji s drugim zemljama (bilateralni, multilateralni) ili partnerima u drugim zemljama? Npr. razmjena informacija, izgradnja kapaciteta, pomoć...	1	Razmjenjujete li informacije na strateškoj razini? Npr. politike na visokoj razini, percepcija rizika...	1	Jesu li nacionalne javne agencije za kibersigurnost u vašoj zemlji uključene u programe međunarodne suradnje?	1	Vodite li rasprave o jednoj ili više tema u okviru multilateralnih sporazuma?	1
	2	Imate li neformalne kanale za suradnju s drugim zemljama?	1	Imate li jedinstvenu točku za kontakt koja može izvršavati funkciju povezivanja kako bi se osigurala prekogranična suradnja s tijelima država članica (skupina za suradnju, mreža timova za odgovor na računalne sigurnosne incidente...)?	1	Razmjenjujete li informacije na taktičkoj razini? Npr. bilten sa subjektima prijetnji, centri za razmjenu i analizu informacija, taktike, tehnike i postupci...	1	Ocjenjujete li redovito ishode inicijativa za međunarodnu suradnju?	1	Vodite li rasprave o jednoj ili više tema u okviru međunarodnih ugovora ili konvencija?	1
	3	Je li državno vodstvo izrazilo namjeru da se uključi u međunarodnu suradnju u području kibersigurnosti?	1	Imate li pojedince koji su osobito angažirani u međunarodnoj suradnji?	1	Razmjenjujete li informacije na operativnoj razini? Npr. informacije o operativnoj koordinaciji, trajni incidenti, IOC-ovi...	1	-		Vodite li rasprave ili pregovore o jednoj ili više tema u okviru međunarodnih skupina stručnjaka? Npr. Globalna komisija za stabilnost kiberprostora (GCSC), ENISA-ina skupina za suradnju za NIS, Skupina vladinih stručnjaka UN-a za informacijsku sigurnost (GGE)...	1
	4	-		-		Sudjelujete li u međunarodnim vježbama u području kibersigurnosti?	1	-		-	
	5	-		-		Sudjelujete li u međunarodnim inicijativama za izgradnju kapaciteta? Npr. osposobljavanje, razvoj vještina, izrada standardnih postupaka...	0	-		-	
	6	-		-		Jeste li sklopili sporazume o uzajamnoj pomoći s drugim zemljama? Npr. aktivnosti agencija za izvršavanje zakonodavstva, sudski postupci, objedinjavanje kapaciteta za odgovor na incidente, dijeljenje sredstava za kibersigurnost...	0	-		-	

Cilj nacionalne strategije za kibersigurnost	#	1. razina	R	2. razina	R	3. razina	R	4. razina	R	5. razina	R
	7	-		-		Jeste li potpisali ili ratificirali međunarodne ugovore ili konvencije u području kibersigurnosti? Npr. Međunarodni kodeks ponašanja za informacijsku sigurnost, Konvencija o kibernetičkom kriminalu ?	0	-		-	

4.2 SMJERNICE ZA PRIMJENU OKVIRA

Cilj je ovog odjeljka pružiti državama članicama određene smjernice i preporuke za uvođenje okvira i ispunjavanje upitnika. Preporuke navedene u nastavku uglavnom proizlaze iz povratnih informacija prikupljenih tijekom razgovora s predstavnicima država članica:

- **Predvidjeti koordinacijske aktivnosti za prikupljanje i konsolidiranje podataka.** Većina država članica potvrđuje da bi provedba takve samoprocjene trebala obuhvaćati oko 15 dana/osoba. Kako bi se provela samoprocjena, morat će se zatražiti velik broj različitih dionika. Stoga se preporučuje da se za fazu pripreme odredi vrijeme za utvrđivanje svih relevantnih dionika u državnim tijelima, javnim agencijama i privatnom sektoru.
- **Utvrditi središnje tijelo zaduženo za dovršetak samoocjenjivanja na nacionalnoj razini.** Budući da bi prikupljanje materijala za sve pokazatelje okvira za procjenu nacionalnih kapaciteta moglo uključivati velik broj dionika, preporučuje se da središnje tijelo ili agencija bude zadužena za dovršetak samoocjenjivanja povezivanjem i koordinacijom sa svim relevantnim dionicima.
- **Upotrebljavati postupak ocjenjivanja kao način za razmjenu informacija o temama povezanima s kibersigurnošću i komunikaciju o njima.** Iskustva koja su države članice stekle pokazala su da su rasprave (bilo u obliku pojedinačnih razgovora ili kolektivnih radionica) dobra prilika za poticanje dijaloga o temama kibersigurnosti te za razmjenu zajedničkih stajališta i područja u kojima su moguća poboljšanja. Osim razjašnjavanja ključnih postignuća, razmjena rezultata može pomoći i u promicanju tema kibersigurnosti.
- **Upotrebljavati nacionalnu strategiju za kibersigurnost za odabir ciljeva koji su predmet procjene.** Sedamnaest ciljeva okvira za procjenu nacionalnih kapaciteta uspostavljeno je na temelju ciljeva koje države članice zajednički obuhvaćaju u svojim nacionalnim strategijama za kibersigurnost. Ciljevi obuhvaćeni nacionalnom strategijom za kibersigurnost trebali bi se upotrebljavati kao sredstvo za utvrđivanje opsega procjene. Međutim, nacionalna strategija za kibersigurnost ne bi trebala ograničiti procjenu. S obzirom na to da je nacionalna strategija za kibersigurnost usmjeren na prioritete, određena se područja namjerno izostavljaju. No to ne znači da određeni kapacitet nije prisutan. Na primjer, ako je određeni cilj izostavljen iz nacionalne strategije za kibersigurnost, ali zemlja ima kapacitete u području kibersigurnosti povezane s tim ciljem, procjena tog cilja može se provesti.
- **Kada se razvije opseg nacionalne strategije za kibersigurnost, potrebno je osigurati da tumačenje ocjena ostane u skladu s razvojem nacionalne strategije za kibersigurnost.** Životni ciklus nacionalne strategije za kibersigurnost višegodišnji je proces. Nacionalne strategije za kibersigurnost nekih država članica obično se provode s trogodišnjim do petogodišnjim planom s promjenama opsega između dvaju uzastopnih izdanja nacionalne strategije za kibersigurnost. U tom je kontekstu potrebno posvetiti posebnu pozornost prikazivanju rezultata samoprocjene dvaju izdanja nacionalne strategije za kibersigurnost: promjene opsega mogu utjecati na konačnu ocjenu zrelosti. Preporučuje se usporedba ocjena za cijeli opseg strateških ciljeva iz godine u godinu (tj. ukupna opća ocjena).

Podsjetnik na mehanizam ocjenjivanja – primjer omjera pokrivenosti

Mehanizam ocjenjivanja uključuje dvije razine ocjena:
(i) **ukupni opći omjer pokrivenosti** na temelju cjelovitog popisa strateških ciljeva prisutnih u okviru za samoprocjenu i
(ii) **ukupni posebni omjer pokrivenosti** koji se temelji na strateškim ciljevima koje je odabrala država članica (obično u skladu s ciljevima iz nacionalne strategije za kibersigurnost određene zemlje).

Osmišljen je tako (vidjeti odjeljak 3.1 o mehanizmu ocjenjivanja) da je ukupni posebni omjer pokrivenosti jednak ili viši od ukupnog omjera opće pokrivenosti jer on kasnije može uključivati

ciljeve koje država članica ne pokriva, čime se smanjuje ukupni opći omjer pokrivenosti. Kada država članica doda novi cilj, povećat će se ukupni omjer pokrivenosti (tj. više obuhvaćenih pokazatelja zrelosti), dok se ukupna posebna zrelost može smanjiti (u slučaju da je novi cilj u početnoj fazi i stoga ima nisku razinu zrelosti).

- **Pri ispunjavanju upitnika za samoprocjenu potrebno je imati na umu da je glavni cilj pružiti potporu državama članicama u izgradnji kapaciteta u području kibersigurnosti.** Stoga se pri ispunjavanju samoprocjene, čak i ako u nekim situacijama može biti teško točno odgovoriti na pitanje, preporučuje odabir odgovora koji je općenito prihvaćen. Ako je, na primjer, odgovor na pitanje u jednom opsegu DA, a u drugom NE, države članice trebale bi imati na umu da odgovor NE zahtijeva djelovanje: plan sanacije ili plan djelovanja u području poboljšanja koji se mora uzeti u obzir u budućem razvoju.

5. SLJEDEĆI KORACI

5.1 BUDUĆA POBOLJŠANJA

Tijekom razgovora s predstavnicima država članica i tijekom faze analize dokumentacije utvrđene su sljedeće preporuke za poboljšanje postojećeg okvira za procjenu nacionalnih kapaciteta kao mogući budući razvoj:

- **Razviti sustav ocjenjivanja kako bi se omogućila veća točnost.** Na primjer, mogao bi se uvesti postotak pokrivenosti umjesto binarnog odgovora DA/NE kako bi se bolje uzela u obzir složenost konsolidacije kapaciteta na nacionalnoj razini. Kao prvi korak odabran je jednostavan pristup s odgovorima DA/NE.
- **Uvesti kvantitativne parametre za mjerenje učinkovitosti nacionalne strategije za kibersigurnost država članica.** Okvir za procjenu nacionalnih kapaciteta usmjeren je na procjenu stupnja zrelosti kapaciteta država članica u području kibersigurnosti. To bi se moglo nadopuniti parametrima za mjerenje djelotvornosti aktivnosti i akcijskih planova koje provode države članice kako bi izgradile te kapacitete. U sadašnjoj fazi nije se činilo realističnim izraditi takve parametre djelotvornosti s obzirom na malo povratnih informacija s terena, poteškoće u pronalaženju smislenih pokazatelja kojima se rezultati povezuju s provedbom nacionalne strategije za kibersigurnost i poteškoće u izradi realističnih pokazatelja koji se mogu naknadno prikupiti. No to ostaje tema budućeg rada.
- **Prijeći s postupka samoprocjene na pristup procjene.** Mogući budući razvoj okvira mogao bi biti pomak prema pristupu procjene kako bi se dosljednije procijenila zrelost kapaciteta država članica u području kibersigurnosti. Ako bi procjenu provodila treća strana, to bi doista moglo omogućiti smanjenje potencijalne pristranosti na najmanju moguću mjeru.

PRILOG A — PREGLED REZULTATA ANALIZE DOKUMENTACIJE

Prilog A sadržava sažetak prethodnog rada ENISA-e na nacionalnoj strategiji za kibersigurnost i pregled relevantnih javno dostupnih modela zrelosti kapaciteta u području kibersigurnosti. Sljedeće pretpostavke uzimaju se u obzir pri odabiru i preispitivanju modela:

- nisu svi modeli utemeljeni na strogoj metodologiji istraživanja;
- struktura i rezultati modela nisu uvijek detaljno objašnjeni s jasnim poveznicama između različitih elemenata svojstvenih svakom modelu;
- neki modeli ne nude detalje o procesu razvoja, strukturi i metodologiji procjene;
- ostali pronađeni modeli i alati ne pružaju nikakve pojedinosti o strukturi i sadržaju te stoga nisu navedeni i
- odabir modela za preispitivanje temelji se na geografskoj pokrivenosti. Naglasak će ponajprije biti na modelima zrelosti u pogledu kapaciteta u području kibersigurnosti koji su izgrađeni kako bi se procijenila uspješnost europskih zemalja. Međutim, važno je proširiti geografsku pokrivenost kako bi se analizirale dobre prakse u izradi modela zrelosti diljem svijeta.

Sustavno preispitivanje relevantnih javno dostupnih modela zrelosti kapaciteta u području kibersigurnosti provedeno je primjenom prilagođenog okvira analize na temelju metodologije koju je Becker definirao za razvoj modela zrelosti.[22] Za svaki postojeći model zrelosti analizirani su sljedeći elementi:

- **naziv modela zrelosti:** naziv modela zrelosti i glavne reference;
- **ustanova:** javna ili privatna ustanova zadužena za oblikovanje modela;
- **opća svrha i cilj:** ukupni opseg modela i planirane ciljne vrijednosti;
- **broj i definicija razina:** broj razina zrelosti modela te njihov opći opis;
- **broj i naziv atributa:** broj i naziv atributa koji se koriste u okviru modela zrelosti. Analiza atributa ima trostruki cilj:
  - raščlaniti model zrelosti na lako razumljive odjeljke;
  - objediniti nekoliko atributa u klastere atributa koji ispunjavaju isti cilj i
  - prikazati različita stajališta o predmetu razine zrelosti.
- **metoda procjene:** metoda procjene modela zrelosti;
- **prikaz rezultata**: definirati metodu vizualizacije za rezultate modela zrelosti. Logika tog koraka temelji se na tome da su modeli zrelosti često neuspješni ako su presloženi i stoga način prikazivanja mora zadovoljiti praktične potrebe.

[22] J. Becker, R. Knackstedt i J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, svezak 1., br. 3, str. 213. – 222., lipanj 2009.
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

Prethodni rad na nacionalnoj strategiji za kibersigurnost

ENISA je 2012. objavila dva dokumenta o temi nacionalnih strategija za kibersigurnost kao dio svojih ranih nastojanja. Prvo, u „Praktičnom vodiču kroz fazu razvoja i provedbe nacionalne strategije za kibersigurnost"[23] predložen je skup konkretnih mjera za učinkovitu provedbu nacionalne strategije za kibersigurnost i predstavljen životni ciklus nacionalne strategije za kibersigurnost u četiri faze: razvoj strategije, provedba strategije, ocjenjivanje strategije i održavanje strategije. Drugo, u dokumentu pod nazivom „Utvrđivanje smjera nacionalnih napora za jačanje sigurnosti u kiberprostoru"[24] opisan je status strategija kibersigurnosti unutar EU-a i šire 2012. i predloženo da države članice odrede zajedničke teme i razlike između svojih nacionalnih strategija za kibersigurnost.

U 2014. objavljen je prvi okvir ENISA-e za ocjenjivanje nacionalne strategije za kibersigurnost neke države članice.[25] Taj okvir sadržava preporuke i dobre prakse, kao i skup alata za izgradnju kapaciteta za procjenu nacionalne strategije za kibersigurnost (npr. utvrđene ciljeve, uložene resurse, ostvarenja, ključne pokazatelje uspješnosti...). Ti se alati pri strateškom planiranju prilagođavaju različitim potrebama zemalja na različitim razinama zrelosti. ENISA je iste godine objavila „Interaktivnu internetsku kartu nacionalnih strategija za kibersigurnost",[26] koja korisnicima omogućuje brz pregled nacionalnih strategija za kibersigurnost svih država članica i zemalja EFTA-e, uključujući njihove strateške ciljeve i dobre primjere provedbe. Karta je najprije izrađena kao repozitorij nacionalnih strategija za kibersigurnost (2014.), a 2018. ažurirana je primjerima provedbe te od 2019. služi kao *informacijski centar* za centralizaciju podataka koje dostavljaju države članice o svojim naporima za poboljšanje nacionalne kibersigurnosti.

U „Vodiču kroz dobre prakse nacionalnih strategija za kibersigurnost"[27] objavljenom 2016. utvrđeno je petnaest strateških ciljeva. U tom se vodiču analizira i stanje provedbe nacionalne strategije za kibersigurnost svake države članice te se utvrđuju različiti nedostatci i izazovi u pogledu te provedbe.

ENISA je 2018.[28] objavila „Nacionalni alat za procjenu strategija za kibersigurnost", interaktivni alat za samoprocjenu kako bi se državama članicama pomoglo da procijene svoje strateške prioritete i ciljeve u vezi s nacionalnom strategijom za kibersigurnost. Tim se alatom putem niza jednostavnih pitanja državama članicama daju konkretne preporuke za provedbu svakog cilja. Naposljetku, u dokumentu „Dobre prakse u inovacijama u području kibersigurnosti u okviru nacionalne strategije za kibersigurnost" objavljenom 2019.[29] predstavljaju se inovacije u području kibersigurnosti u okviru nacionalne strategije za kibersigurnost. U dokumentu se navode izazovi i dobre prakse u različitim dimenzijama inovacija, kako ih doživljavaju stručnjaci za predmetno područje, kao pomoć u izradi budućih inovativnih strateških ciljeva.

[23] Nacionalna strategija za kibersigurnost: Praktični vodič kroz razvoj i izvršenje (ENISA, 2012.)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] Nacionalna strategija za kibersigurnost: Utvrđivanje smjera nacionalnih napora za jačanje sigurnosti u kiberprostoru (ENISA, 2012.)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] Okvir za procjenu nacionalne strategije za kibersigurnost (ENISA, 2014.)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] Nacionalne strategije za kibersigurnost – interaktivna karta (ENISA, 2014., ažurirana 2019.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Ovim se dokumentom ažurira vodič iz 2012.: Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost: Osmišljavanje i provedba nacionalnih strategija za kibersigurnost (ENISA, 2016.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Alat za procjenu nacionalnih strategija za kibersigurnost (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

A.1 Model zrelosti kapaciteta u području kibersigurnosti za države (CMM)

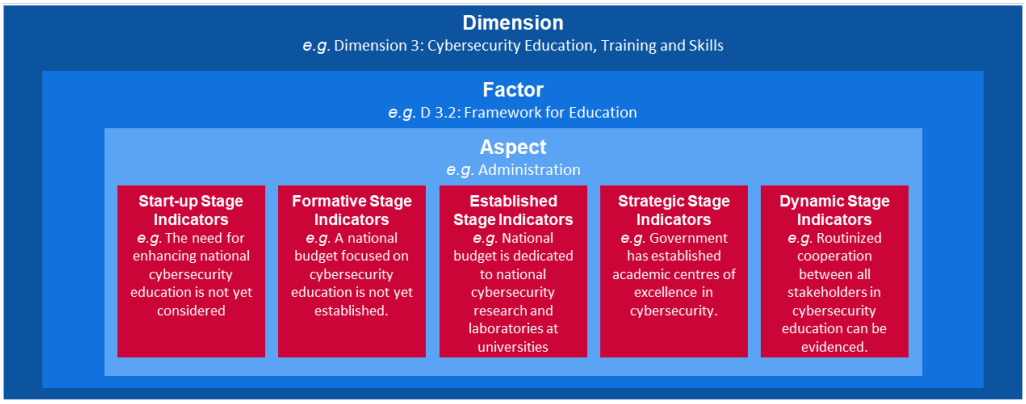
Model zrelosti kapaciteta u području kibersigurnosti za države (CMM) razvio je Globalni centar za kapacitete u području kibersigurnosti (Centar za kapacitete), dio instituta Oxford Martin School u okviru Sveučilišta u Oxfordu. Cilj je Centra za kapacitete povećati opseg i djelotvornost izgradnje kapaciteta u području kibersigurnosti, kako u Ujedinjenoj Kraljevini tako i na međunarodnoj razini, uvođenjem modela zrelosti kapaciteta u području kibersigurnosti (CMM). Model CMM izravno je usmjeren na zemlje koje žele povećati svoje nacionalne kapacitete u području kibersigurnosti. Model je prvotno uveden 2014., a revidiran je 2016. nakon što je upotrijebljen za preispitivanje 11 nacionalnih kapaciteta u području kibersigurnosti.

Atributi/dimenzije

U okviru modela CMM smatra se da kapacitet kibersigurnosti obuhvaća **pet dimenzija** koje predstavljaju klastere kapaciteta u tom području. Svaki klaster predstavlja različite istraživačke „prizme" s pomoću kojih se kapacitet u području kibersigurnosti može proučiti i razumjeti. U okviru pet dimenzija pojedinosti o posjedovanju kapaciteta u području kibersigurnosti opisuju se **čimbenicima**. Te su pojedinosti elementi koji pridonose povećanju zrelosti kapaciteta u području kibersigurnosti u svakoj dimenziji. Za svaki čimbenik postoji nekoliko **aspekata** koji predstavljaju različite sastavne dijelove čimbenika. Aspekti su organizacijska metoda podjele pokazatelja na manje klastere koje je lakše razumjeti. Svaki se aspekt zatim ocjenjuje s pomoću **pokazatelja** kako bi se opisali koraci, mjere ili sastavnice koji upućuju na određenu fazu zrelosti (definiranu u odjeljku u nastavku) u okviru posebnog aspekta, čimbenika i dimenzije.

Prethodno navedeni pojmovi mogu biti slojeviti kako je prikazano na slici u nastavku.

Slika 4.: Primjer pokazatelja CMM-a



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimenzija npr. 3. dimenzija Obrazovanje, osposobljavanje i vještine u području kibersigurnosti
Factor e.g. D 3.2: Framework for Education	Čimbenik npr. D 3.2: Okvir za obrazovanje
Aspect e.g. Administration	Aspekt npr. uprava
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Pokazatelji početne faze npr. poboljšanje obrazovanja u području kibersigurnosti na nacionalnoj razini još se ne razmatra

Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Pokazatelji faze razvoja npr. još nije utvrđen nacionalni proračun usmjeren na obrazovanje u području kibersigurnosti
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Pokazatelj faze utvrđivanja npr. nacionalni proračun namijenjen je istraživanjima i laboratorijima u području kibersigurnosti na sveučilištima na nacionalnoj razini
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Pokazatelji strateške faze npr. vlada je uspostavila akademski centar izvrsnosti u vezi s obrazovanjem u području kibersigurnosti
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Pokazatelji dinamične faze npr. rutinska suradnja svih dionika

Pet dimenzija detaljno je opisano u nastavku:

i osmišljavanje politike i strategije u području kibersigurnosti (6 čimbenika);
ii poticanje odgovorne kulture kibersigurnosti u društvu (5 čimbenika);
iii razvoj znanja o kibersigurnosti (3 čimbenika);
iv uspostava djelotvornih pravnih i regulatornih okvira (3 čimbenika);
v kontroliranje rizika s pomoću normi, organizacija i tehnologija (7 čimbenika).

Razine zrelosti

U okviru modela CMM upotrebljava se **5 razina zrelosti** kako bi se utvrdilo u kojoj je mjeri zemlja ostvarila napredak u odnosu na određeni čimbenik/aspekt kapaciteta u području kibersigurnosti. Te razine služe kao prikaz postojećeg kapaciteta u području kibersigurnosti:

- **početna razina**: u ovoj fazi ili ne postoji zrelost kibersigurnosti ili je tek u začetku. Možda će se održati početne rasprave o izgradnji kapaciteta u području kibersigurnosti, ali nisu poduzete konkretne mjere. U ovoj fazi nema vidljivih dokaza;
- **razina razvoja**: neke značajke aspekata počele su rasti i formuliraju se, ali mogu biti *ad hoc*, neorganizirane, loše definirane ili jednostavno „nove”. Međutim, dokazi o toj aktivnosti mogu se jasno predstaviti;
- **razina utvrđivanja**: elementi tog aspekta uspostavljeni su i funkcioniraju. Međutim, ne postoji dobro promišljeno razmatranje relativne raspodjele sredstava. U pogledu „relativnih” ulaganja u različite elemente tog aspekta donesen je mali broj kompromisnih odluka. Međutim, taj je aspekt funkcionalan i definiran;
- **strateška razina**: donesene su odluke o tome koji su dijelovi aspekta važni i koji su manje važni za određenu organizaciju ili državu. Strateška faza odražava činjenicu da su ti izbori doneseni ovisno o posebnim okolnostima u državi ili organizaciji;
- **dinamična razina**: u ovoj fazi postoje jasni mehanizmi za izmjenu strategije ovisno o prevladavajućim okolnostima kao što su tehnologija okruženja prijetnji, globalni sukob ili značajna promjena u jednom problematičnom području (npr. kiberkriminalitet ili privatnost). Dinamične organizacije razvile su napredne metode za promjenu strategija. Ova faza odlikuje se brzim donošenjem odluka, preraspodjelom resursa i stalnom pozornošću koja se posvećuje okruženju koje se mijenja.

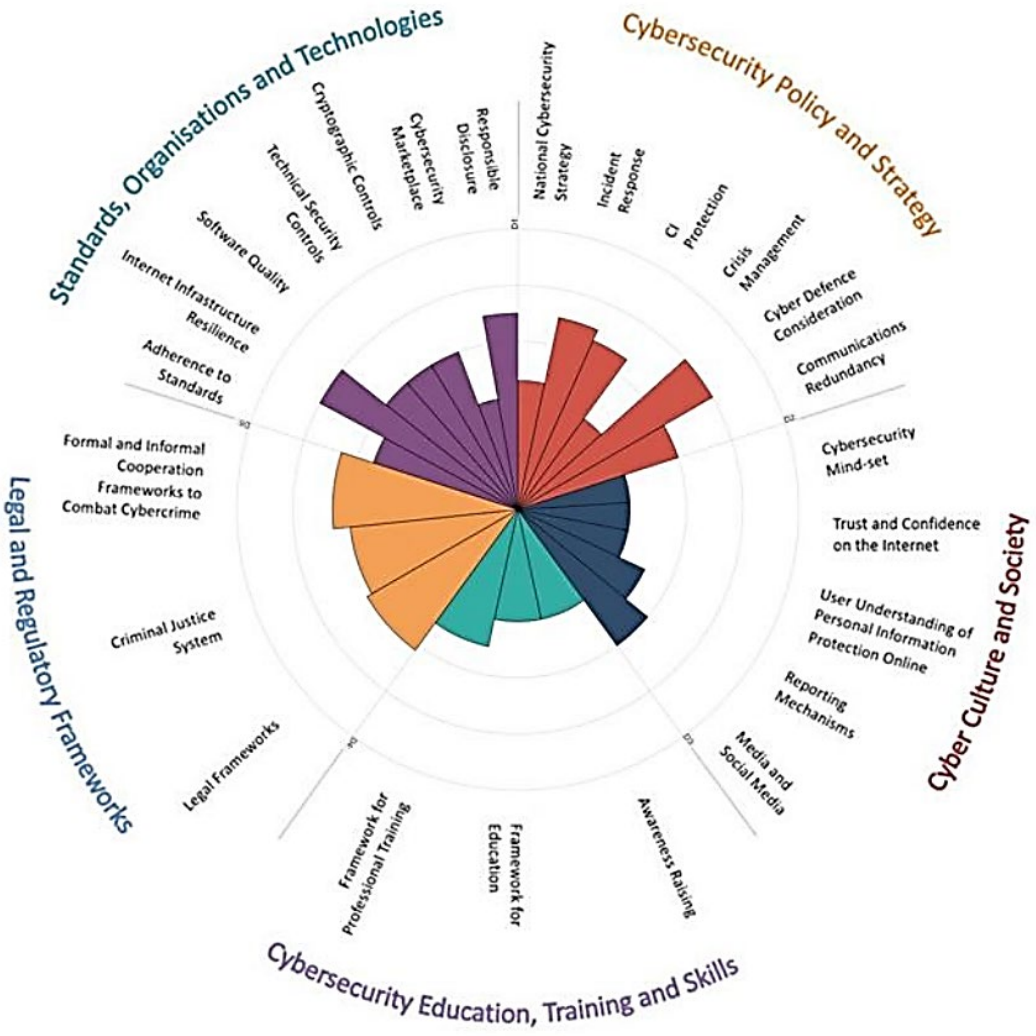
Metoda procjene

Budući da Centar za kapacitete nema temeljito i dubinsko razumijevanje svakog domaćeg konteksta u kojem se model primjenjuje, surađuje s međunarodnim organizacijama, ministarstvima domaćinima ili organizacijama u dotičnoj zemlji kako bi preispitao zrelost kapaciteta u području kibersigurnosti. Kako bi se procijenila razina zrelosti pet dimenzija uključenih u CMM, Centar za kapacitete i organizacija domaćin sastaju se s relevantnim nacionalnim dionicima iz javnog i privatnog sektora tijekom dva ili tri dana kako bi organizirali fokusne skupine o dimenzijama CMM-a. O svakoj dimenziji najmanje dvaput raspravljaju različiti klasteri dionika. To služi kao preliminarni skup podataka za naknadnu procjenu.

Način ili prikaz rezultata

Model zrelosti kapaciteta u području kibersigurnosti pruža pregled razine zrelosti svake zemlje s pomoću radara koji se sastoji od pet odjeljaka, po jedan za svaku dimenziju. Svaka dimenzija predstavlja petinu grafičkog prikaza, pri čemu pet faza zrelosti za svaki čimbenik izlazi iz središta grafičkog prikaza. Kao što je prikazano u nastavku, „početak" je najbliži središtu grafičkog prikaza, dok je „dinamični" aspekt na rubu.

Slika 5. Model CMM: Pregled rezultata



Standards, Organisations and Technologies	Norme, organizacije i tehnologija
Legal Regulatory Frameworks	Pravni regulatorni okviri
Cybersecurity Education, Training and Skills	Obrazovanje, osposobljavanje i vještine u području kibersigurnosti
Cybersecurity Policy and Strategy	Politika i strategija u području kibersigurnosti
Cyber Culture and Society	Kiberkultura i kiberdruštvo
Responsible Disclosure	Odgovorno objavljivanje
Cybersecurity market place	Tržište kibersigurnosti
Cryptographic Controls	Kriptografske kontrole
Technical Security Controls	kontrole tehničke sigurnosti
Software Quality	Kvaliteta softvera
Internet Infrastructure Resilience	Otpornost internetske infrastrukture
Adherence to Standards	Pridržavanje normi
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formalni i neformalni okviri za suradnju u borbi protiv kiberkriminaliteta
Criminal Justice System	Kaznenopravni sustav
Legal Frameworks	Pravni okviri
Framework for Professional Training	Okvir za stručno usavršavanje
Framework for Education	Okvir za obrazovanje
Awareness Raising	Podizanje svijesti
Media and Social Medai	Mediji i društveni mediji

Reporting Mechanisms	Mehanizmi izvješćivanja
User Understanding of Personal Information Protection Online	Korisničko razumijevanje zaštite osobnih informacija na internetu
Trust and Confidence on the Internet	Pouzdanje i povjerenje na internetu
Cybersecurity Mind-set	Način razmišljanja usmjeren na kibersigurnost
Communications Redundancy	Redundantnost komunikacije
Cyber Defence Consideration	Razmatranje kiberobrane
Crisis Management	Upravljanje krizom
CI Protection	Zaštita ključne infrastrukture
Incident Response	Odgovor na incidente
National Cybersecurity Strategy	Nacionalna strategija za kibersigurnost

Globalni centar za kapacitete u području kibersigurnosti pri institutu Oxford Martin School, Sveučilište u Oxfordu, 2017.

A.2 Model zrelosti kapaciteta u području kibersigurnosti (C2M2)

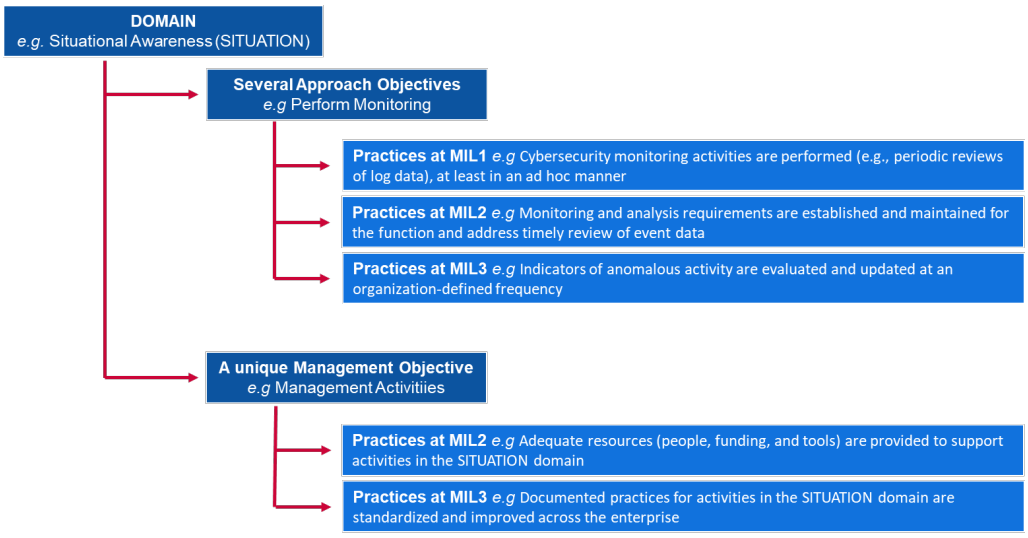
Model zrelosti kapaciteta u području kibersigurnosti (C2M2) razvilo je Ministarstvo energetike SAD-a u suradnji sa stručnjacima iz privatnog i javnog sektora. Cilj je Centra za kapacitete pomoći organizacijama svih sektora, vrsta i veličina u procjeni i poboljšanju svojih programa kibersigurnosti te jačanju njihove operativne otpornosti. Model C2M2 usmjeren je na provedbu kibersigurnosnih praksi povezanih s informacijama, informacijskom tehnologijom (IT) te operativnom tehnologijom (OT) i upravljanje njima te na okruženja u kojima djeluju. C2M2 definira modele kao: „skup značajki, atributa, pokazatelja ili uzoraka koji predstavljaju sposobnost i napredak u određenoj disciplini". Model C2M2 prvotno je uveden 2014., a revidiran je 2019.

Atributi/dimenzije

U okviru modela C2M2 razmatra se **deset domena** koje predstavljaju logičko grupiranje praksi u području kibersigurnosti. Svaki skup praksi predstavlja aktivnosti koje organizacija može obavljati kako bi uspostavila i postigla zrelost kapaciteta u tom području. Svaka domena zatim je povezana s **jedinstvenim ciljem upravljanja** i **nekoliko ciljeva pristupa**. U okviru ciljeva pristupa i upravljanja detaljno je opisano **nekoliko praksi** kako bi se opisale institucionalizirane aktivnosti.

Odnos između tih pojmova sažet je u nastavku:

Slika 6.: Primjer pokazatelja modela C2M2



Domain eg Situational Awareness (SITUATION)	**Domena** npr. informiranost o stanju (SITUACIJA)
Several Approaches Objectives e.g. Perform Monitoring	**Nekoliko ciljeva pristupa** npr. praćenje
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Prakse na 1. razini zrelosti pokazatelja** npr. provode se aktivnosti praćenja kibersigurnosti (npr. periodični pregledi podataka iz evidencije), barem na *ad hoc* način

Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency
A unique Management Objectve e.g. Management Activities
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise

Prakse na 2. razini zrelosti pokazatelja npr. zahtjevi u pogledu praćenja i analize utvrđeni su i održavaju se za funkciju i odnose se na pravovremeno preispitivanje podataka o događaju
Prakse na 3. razini zrelosti pokazatelja npr. pokazatelji neuobičajene aktivnosti ocjenjuju se i ažuriraju učestalošću koju je odredila organizacija. Jedinstveni cilj upravljanja, npr. aktivnosti upravljanja
Prakse na 2. razini zrelosti pokazatelja npr. odgovarajući resursi (ljudi, financijska sredstva i alati) za potporu aktivnostima u domeni SITUACIJA
Prakse na 3. razini zrelosti pokazatelja npr. dokumentirane prakse za aktivnosti u domeni SITUACIJA normirane su i poboljšane u cijelom poduzeću.

U nastavku je navedeno deset domena:

i upravljanje rizikom (RIZIK);
ii upravljanje imovinom, promjenama i konfiguracijom (IMOVINA);
iii upravljanje identitetom i pristupom (PRISTUP);
iv upravljanje prijetnjama i ranjivošću (PRIJETNJA);
v informiranost o stanju (SITUACIJA);
vi odgovor na događaje i incidente (ODGOVOR);
vii upravljanje lancem opskrbe i vanjskim ovisnostima (OVISNOSTI);
viii upravljanje radnom snagom (RADNA SNAGA);
ix arhitektura kibersigurnosti (ARHITEKTURA) i
x upravljanje programom kibersigurnosti (PROGRAM).

Razine zrelosti

U modelu C2M2 upotrebljavaju se **četiri razine zrelosti** (koje se nazivaju razine zrelosti pokazatelja – MIL) za utvrđivanje dvostrukog napretka u pogledu zrelosti: napredak u pristupu i napredak u upravljanju. Razine zrelosti pokazatelja kreću se od 0. do 3. i trebale bi se primjenjivati zasebno za svaku domenu.

- **0. razina zrelosti pokazatelja**: prakse se ne provode.
- **1. razina zrelosti pokazatelja**: početne se prakse provode, ali mogu biti *ad hoc*.
- **2. razina zrelosti pokazatelja**: značajke upravljanja:
  - prakse se dokumentiraju;
  - osigurani su odgovarajući resursi za potporu procesu;
  - osoblje koje provodi prakse posjeduje odgovarajuće vještine i znanje i
  - dodijeljene su odgovornosti i ovlasti za provedbu prakse.

  Značajka pristupa:
  - prakse su potpunije ili naprednije nego na 1. razini zrelosti pokazatelja.
- **3. razina zrelosti pokazatelja**: značajke upravljanja:
  - aktivnosti se vode politikama (ili drugim organizacijskim direktivama);
  - ciljevi uspješnosti za aktivnosti u okviru domene utvrđeni su i prate se kako bi se pratila postignuća i
  - dokumentirane prakse za aktivnosti u okviru domene normirane su i poboljšane u cijelom poduzeću.

  Značajka pristupa:
  - prakse su potpunije ili naprednije nego na 2. razini zrelosti pokazatelja.

Metoda procjene

C2M2 osmišljen je za upotrebu s pomoću **metodologije za samoocjenjivanje** i skupa alata (dostupnog na zahtjev) kako bi organizacija mogla mjeriti i poboljšavati svoj program u području kibersigurnosti. Samoprocjena s pomoću skupa alata može se dovršiti za jedan dan, no skup alata mogao bi se prilagoditi strožim procjenama. Osim toga, C2M2 može poslužiti kao smjernica za razvoj novog programa kibersigurnosti.

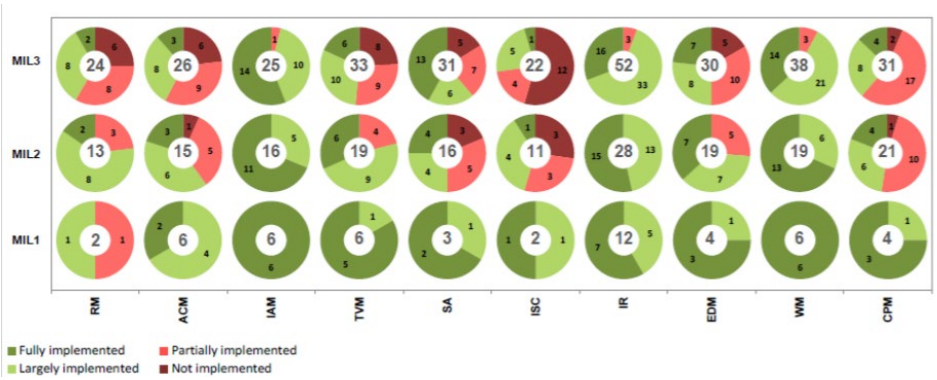
Sadržaj modela prikazan je na visokoj razini apstrakcije kako bi ga mogle protumačiti organizacije različitih vrsta, struktura, veličina te industrije. Širokim korištenjem modela u određenom sektoru može se podržati uspoređivanje kapaciteta sektora u području kiberisgurnosti u odnosu na referentne vrijednosti.

Način ili prikaz rezultata

Model C2M2 sadržava izvješće o ocjenjivanju koje se temelji na rezultatima istraživanja. U izvješću se rezultati prikazuju s na dva načina: objektivni prikaz, koji sadržava odgovore svake domene i njezine ciljeve, te prikaz domene, koji sadržava odgovore svih domena i razine zrelosti pokazatelja. Oba prikaza temelje se na sustavu prikaza koji karakteriziraju tortni grafikoni, jedan za svaki odgovor, i mehanizam semafora za ocjenjivanje. Kao što je prikazano na slici 7., crvena područja na kružnom grafikonu pokazuju broj pitanja na koja je odgovoreno „nije provedeno" (tamnocrveno) ili „djelomično provedeno" (svijetlocrveno). Zelena područja pokazuju broj pitanja na koje je odgovoreno „većinom provedeno" (svijetlozeleno) ili „u cijelosti provedeno" (tamnozeleno).

Na slici 7. u nastavku nalazi se primjer kartice za ocjenjivanje na kraju procjene zrelosti. Na osi X nalazi se deset domena modela C2M2, a na osi Y prikazane su razine zrelosti (MIL). Promatrajući grafikon i s obzirom na domenu upravljanja rizikom (RM), moguće je uočiti tri tortna grafikona od kojih jedan odgovara svakoj razini zrelosti MIL1, MIL2 i MIL3. Za domenu RM u grafikonu ističe se da postoje dvije stavke koje treba ocijeniti radi postizanja prve razine zrelosti, MIL1. U tom je slučaju jedna ocjena „većinom provedeno" i jedna ocjena „djelomično provedeno". Za drugu razinu zrelosti, MIL2, model predviđa 13 stavki koje treba ocijeniti. Dvije od tih 13 stavki pripadaju prvoj razini, MIL1, a 11 drugoj razini, MIL2. Isto se odnosi i na treću razinu, MIL3.

Slika 7: C2M2 – Primjer prikaza domene



Fully implemented	U cijelosti provedeno
Largely implemented	Većinom provedeno
Partially implemented	Djelomično provedeno
Not implemented	Nije provedeno
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

Izvor: Ministarstvo energetike SAD-a, Ured za isporuku električne energije i energetsku pouzdanost, 2015.

A.3 Okvir za poboljšanje kibersigurnosti ključne infrastrukture

Okvir za poboljšanje kibersigurnosti ključne infrastrukture razvijen je u okviru Nacionalnog instituta za norme i tehnologiju (NIST). Naglasak je na usmjeravanju aktivnosti u području kibersigurnosti i upravljanju rizicima unutar organizacije. Namijenjen je svim vrstama organizacija bez obzira na veličinu, stupanj kibersigurnosnog rizika ili sofisticiranost kibersigurnosti. S obzirom na to da je riječ o okviru, a ne o modelu, osmišljen je drukčije nego prethodno analizirani modeli.

Okvir se sastoji od tri dijela: temelj okvira, redovi provedbe i profili okvira:

- **Temelj okvira** skup je aktivnosti u području kibersigurnosti, željenih ishoda i primjenjivih referenci koje su zajedničke u svim sektorima ključne infrastrukture. One su slične atributima ili dimenzijama koji se nalaze u modelima zrelosti kapaciteta u području kibersigurnosti.
- **Redovi provedbe okvira** („redovi”) pružaju kontekst o tome kako organizacija gleda na kibersigurnosne rizike i postupke uspostavljene za upravljanje tim rizikom. U rasponu od djelomičnog (1. red) do prilagodljivog (4. red), redovi opisuju sve veći stupanj strogosti i sofisticiranosti praksi upravljanja rizicima u području kibersigurnosti. Redovi ne predstavljaju razine zrelosti, već su namijenjeni za potporu donošenju organizacijskih odluka o tome kako upravljati kibersigurnosnim rizicima, kao i o tome koje su dimenzije organizacije više prioritetne i mogle bi dobiti dodatne resurse.
- **Profil okvira** („profil”) predstavlja rezultate koji se temelje na poslovnim potrebama koje je organizacija odabrala iz kategorija i potkategorija okvira. Profil se može opisati u pogledu usklađivanja normi, smjernica i praksi s temeljem okvira u određenom scenariju provedbe. Profili se mogu upotrebljavati za utvrđivanje mogućnosti za poboljšanje kibersigurnosnog položaja usporedbom „postojećeg” profila (stanje „kako jest”) s „ciljanim” profilom (status quo).

Temelj okvira

Temelj okvira sastoji se od pet **funkcija**. Ako ih se razmatra zajedno, te funkcije pružaju strateški pregled životnog ciklusa upravljanja kibersigurnosnim rizicima organizacije. U temelju okvira zatim se utvrđuju temeljne ključne **kategorije** i **potkategorije** za svaku funkciju te ih se usklađuje s primjerom informativnih referentnih podataka kao što su postojeće norme, smjernice i prakse za svaku potkategoriju.

Funkcije i kategorije navedene su u nastavku:

i **utvrđivanje**: razviti organizacijsko razumijevanje o tome kako upravljati kibersigurnosnim rizicima za sustave, ljude, imovinu, podatke i kapacitete.
- Potkategorije: upravljanje imovinom, poslovno okruženje, upravljanje, procjena rizika i strategija upravljanja rizikom

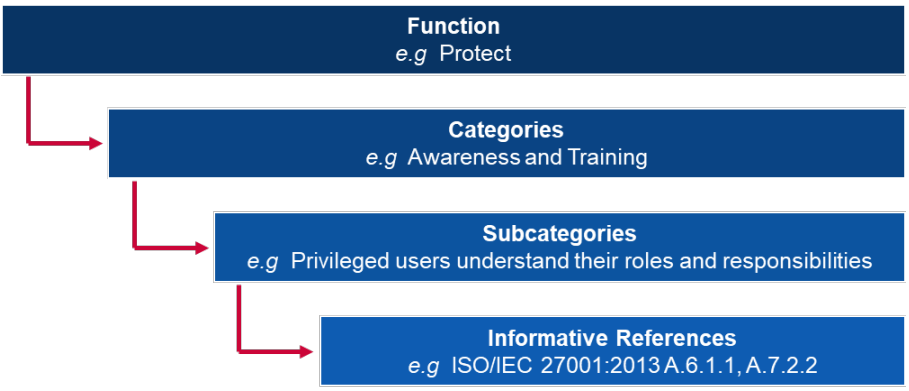
ii **zaštita**: razviti i provesti odgovarajuće zaštitne mjere kako bi se osiguralo pružanje ključnih usluga.
- Potkategorije: upravljanje identitetom i kontrola pristupa, informiranost i osposobljavanje, sigurnost podataka, procesi i postupci zaštite informacija, održavanje, zaštitna tehnologija

iii **otkrivanje**: razviti i provoditi odgovarajuće aktivnosti za utvrđivanje događaja povezanog s kibersigurnošću.
- Potkategorije: neuobičajene aktivnosti i događaji, stalno praćenje sigurnosti i procesi otkrivanja.

iv **odgovor**: razviti i provoditi odgovarajuće aktivnosti za poduzimanje mjera u pogledu otkrivenog kiberincidenta.
- Potkategorije: planiranje odgovora, komunikacija, analiza, ublažavanje i poboljšanja.

v **oporavak**: razviti i provoditi odgovarajuće aktivnosti za održavanje planova za otpornost i za ponovnu uspostavu svih kapaciteta ili usluga koje su pretrpjele štetu zbog kiberincidenta.
- Potkategorije: planiranje oporavka, poboljšanja i komunikacija

Slika 8.: Primjer okvira za poboljšanje kibersigurnosti ključne infrastrukture



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

Funkcija npr. zaštita
Kategorije npr. informiranost i osposobljavanje
Potkategorije npr. privilegirani korisnici razumiju svoje uloge i odgovornosti

Informativne reference npr. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Redovi

Okvir za poboljšanje kibersigurnosti ključne infrastrukture oslanja se na **četiri reda**, od kojih je svaki definiran na tri osi: postupak upravljanja rizikom, integrirani program upravljanja rizikom i vanjsko sudjelovanje. Redovi se ne smatraju razinama zrelosti, već okvirom kojim se organizacijama omogućuje kontekstualizacija njihovih stajališta o kibersigurnosnom riziku i postupcima koji su uspostavljeni za upravljanje tim rizikom.

- **1. red: djelomično**
  - **Postupak upravljanja rizicima**: organizacijske prakse upravljanja rizicima u području kibersigurnosti nisu formalizirane, a rizicima se upravlja na *ad hoc* osnovi i katkad na reaktivan način;
  - **integrirani program upravljanja rizikom**: svijest o kibersigurnosnom riziku na organizacijskoj razini ograničena je. Organizacija provodi upravljanje rizicima u području kibersigurnosti na nepravilan način i na pojedinačnoj osnovi te možda nema postupke kojima se omogućuje razmjena informacija o kibersigurnosti unutar organizacije;
  - **vanjsko sudjelovanje**: organizacija ne razumije svoju ulogu u širem ekosustavu u pogledu svojih ovisnosti ili ovisnih elemenata. Organizacija općenito nije svjesna kiberrizika u lancu opskrbe povezanih s proizvodima i uslugama koje pruža i koje upotrebljava;
- **2. red: informiranost o riziku**
  - **Postupak upravljanja rizikom**: prakse upravljanja rizicima odobrava rukovodstvo, ali se ne mogu utvrditi kao politika na razini organizacije;
  - **integrirani program upravljanja rizikom**: postoji svijest o kibersigurnosnom riziku na organizacijskoj razini, ali nije uspostavljen organizacijski pristup upravljanju kibersigurnosnim rizicima. Provodi se procjena rizika za kibersigurnost organizacijske i vanjske imovine, ali obično nije ponovljiva;
  - **vanjsko sudjelovanje**: organizacija općenito razumije svoju ulogu u širem ekosustavu u pogledu svojih ovisnosti ili ovisnih elemenata, ali ne oboje. Osim toga, organizacija je svjesna kiberrizika u lancu opskrbe opskrbe povezanih s proizvodima i uslugama koje pruža i koristi, ali ne djeluje dosljedno ili formalno na te rizike;
- **3. red: ponovljivo**
  - **Postupak upravljanja rizikom**: prakse upravljanja rizicima organizacije službeno su odobrene i izražene kao politika. Organizacijske prakse u području kibersigurnosti redovito se ažuriraju na temelju primjene postupaka upravljanja rizicima na promjene u zahtjevima poslovanja/nadležnosti te promjenjivih prijetnji i tehnologije;

- **integrirani program upravljanja rizikom**: postoji pristup upravljanju rizicima u području kibersigurnosti na razini organizacije. Politike, procesi i postupci koji se temelje na informacijama o riziku definiraju se, provode kako je predviđeno i preispituju. Viši rukovoditelji osiguravaju da se kibersigurnost uzima u obzir u svim područjima djelovanja organizacije;
- **vanjsko sudjelovanje**: organizacija razumije svoju ulogu, ovisnosti i ovisne elemente u širem ekosustavu te može pridonijeti boljem razumijevanju rizika u zajednici. Organizacija je svjesna kiberrizika u lancu opskrbe povezanih s proizvodima i uslugama koje pruža i koristi;

▶ **4. red: prilagodljivo**

- **Postupak upravljanja rizikom**: organizacija prilagođava svoje prakse u području kibersigurnosti na temelju prethodnih i postojećih kibersigurnosnih aktivnosti, uključujući stečena iskustva i prediktivne pokazatelje;
- **integrirani program upravljanja rizikom**: postoji pristup upravljanju kibersigurnosnim rizikom na razini organizacije koji se zasniva na politikama, procesima i postupcima utemeljenima na riziku za suočavanje s mogućim kibersigurnosnim događajima i
- **vanjsko sudjelovanje**: organizacija razumije svoju ulogu, ovisnosti i ovisne elemente u širem ekosustavu te može pridonijeti širem razumijevanju rizika u zajednici.

Metoda procjene

Okvir za poboljšanje kibersigurnosti ključne infrastrukture namijenjen je organizacijama u cilju samoprocjene rizika kako bi svoj pristup kibersigurnosti i ulaganja učinile racionalnijima, djelotvornijima i vrednijima. Kako bi se ispitala djelotvornost ulaganja, organizacija prvo mora jasno razumjeti svoje organizacijske ciljeve, odnos između tih ciljeva i poticajne ishode u pogledu kibersigurnosti. Ishodima u pogledu kibersigurnosti sadržanima u temelju okvira podržava se samoprocjena djelotvornosti ulaganja i aktivnosti u području kibersigurnosti.

A.4 Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2)

Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2) razvio je 2018. Pravni fakultet Sveučilišta u Kataru. Model Q-C2M2 temelji se na različitim postojećim modelima za izradu sveobuhvatne metodologije procjene kako bi se poboljšao okvir za kibersigurnost Katara.

Atributi/dimenzije

U modelu Q-C2M2 primjenjuje se pristup iz okvira Nacionalnog instituta za norme i tehnologiju (NIST) u skladu s kojim se pet osnovnih funkcija upotrebljava kao glavne domene modela. Pet osnovnih funkcija primjenjivo je u katarskom kontekstu jer su zajedničke u svim sektorima ključne infrastrukture, što je važan element u okviru za kibersigurnost Katara. Model Q-C2M2 temelji se na **pet domena**, a svaka se domena zatim dijeli na nekoliko **poddomena** kako bi se obuhvatio cijeli raspon zrelosti kapaciteta u području kibersigurnosti.

U nastavku se navodi pet domena:

i **domena razumijevanja** obuhvaća četiri poddomene: kiberupravljanje, imovina, rizici i osposobljavanje;
ii **poddomene** u okviru **domene** sigurnosti obuhvaćaju sigurnost podataka, sigurnost tehnologije, sigurnost pristupa, sigurnost komunikacije i sigurnost osoblja;
iii **domena izlaganja** obuhvaća poddomene praćenja, upravljanja incidentima, otkrivanja, analize i izloženosti;
iv **domena odgovora** obuhvaća planiranje odgovora, ublažavanje i komunikaciju odgovora i
v **domena održavanja** obuhvaća planiranje oporavka, upravljanje kontinuitetom, poboljšanje i vanjske ovisnosti.

Razine zrelosti

U modelu Q-C2M2 upotrebljava se **pet razina zrelosti** kojima se mjeri zrelost kapaciteta državnog subjekta ili nedržavne organizacije na razini osnovne funkcije. Te su razine usmjerene na procjenu zrelosti u pet domena navedenih u prethodnom odjeljku.

- **Početak**: u nekim se domenama primjenjuju *ad hoc* prakse i postupci u području kibersigurnosti;
- **Provedba**: donesene su politike za provedbu svih aktivnosti u području kibersigurnosti u domenama s ciljem dovršetka provedbe u određenom trenutku;
- **Razvoj**: provedene su politike i prakse za razvoj i poboljšanje aktivnosti u području kibersigurnosti u domenama s ciljem predlaganja novih aktivnosti za provedbu;
- **Prilagodljivost**: preispituju se i pregledavaju aktivnosti u području kibersigurnosti te usvajaju prakse na temelju prediktivnih pokazatelja koji proizlaze iz prethodnih iskustava i mjera i
- **Brzina**: nastavlja se s provedbom prilagodljive faze s dodatnim naglaskom na brzini i agilnosti pri provedbi aktivnosti u domenama.

Metoda procjene

Model Q-C2M2 u ranoj je fazi istraživanja i još nije spreman za provedbu. Riječ je okviru koji bi se u budućnosti mogao upotrijebiti za uvođenje detaljnog modela procjene za katarske organizacije.

A.5 Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)

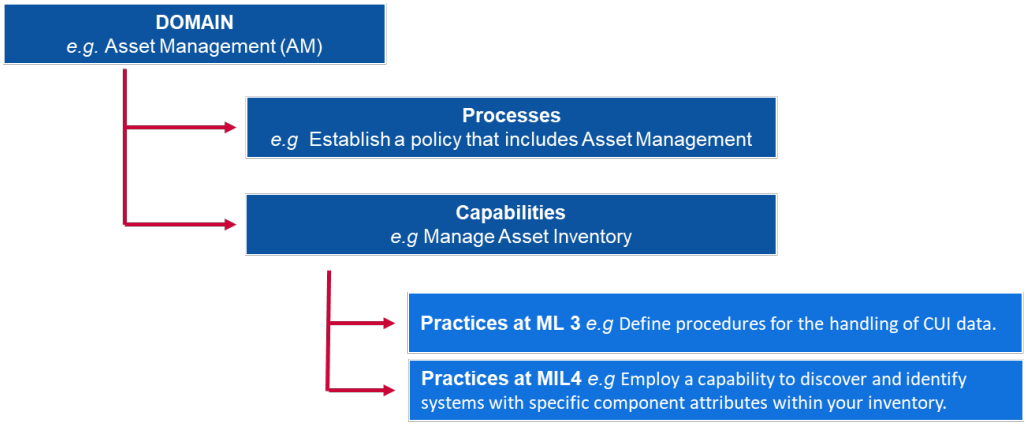
Certifikaciju modela zrelosti kapaciteta u području kibersigurnosti (CMMC) razvilo je Ministarstvo obrane SAD-a u suradnji sa Sveučilištem Carnegie Mellon i laboratorijem za primijenjenu fiziku Sveučilišta Johns Hopkins. Glavni je cilj Ministarstva obrane u izradi tog modela zaštita informacija iz sektora obrane i industrije (DIB). Informacije na koje se odnosi model CMMC klasificirane su kao „savezne ugovorne informacije”, koje vlada pruža ili koje su dobivene za nju na temelju ugovora te koje nisu namijenjene javnoj objavi, ili „kontrolirane neklasificirane informacije”, koje zahtijevaju zaštitne kontrole ili kontrole objavljivanja u skladu sa zakonima, propisima i vladinim politikama te su u skladu s njima. Modelom CMMC mjeri se zrelost kibersigurnosti i pruža najbolja praksa zajedno s elementom certificiranja kako bi se osigurala provedba praksi povezanih sa svakom razinom zrelosti. Najnovija inačica CMMC-a objavljena je 2020. godine.

Atributi/dimenzije

CMMC sadržava **sedamnaest domena** koje predstavljaju klastere procesa i kapaciteta u području kibersigurnosti. Svaka se domena zatim raščlanjuje na više **procesa** koji su slični u različitim domenama te jedan ili više **kapaciteta** koje obuhvaćaju pet razina zrelosti. Jedan ili više kapaciteta zatim se detaljno razrađuju u **prakse** za svaku relevantnu razinu zrelosti.

Odnos između tih pojmova je sljedeći:

Slika 9.: Primjer pokazatelja CMMC-a



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

DOMENA npr. upravljanje imovinom (AM)
Postupci
npr. uspostava politike koja obuhvaća upravljanje imovinom
Sposobnosti
npr. upravljanje inventarom imovine
Prakse na 3. razini zrelosti npr. utvrđivanje postupaka za podatke u okviru CUI-ja
Prakse na 4. razini zrelosti npr. mogućnost otkrivanja i utvrđivanja sustava s posebnim atributima komponenata u inventaru

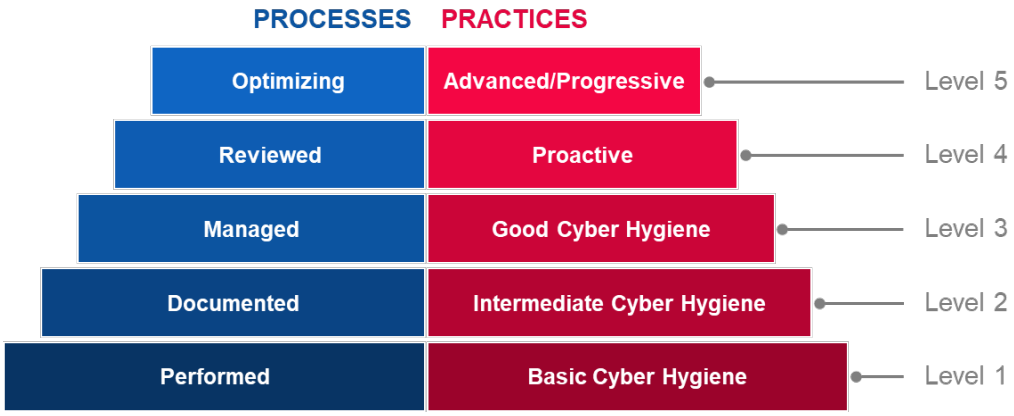
Sedamnaest domena navedeno je u nastavku:

i kontrola pristupa (AC);
ii upravljanje imovinom (AM);
iii revizija i odgovornost (AU);
iv informiranost i osposobljavanje (AT);
v upravljanje konfiguracijom (CM);
vi identifikacija i autentifikacija (IA);
vii odgovor na incidente (IR);
viii održavanje (MA);
ix zaštita medija (MP);
x sigurnost osoblja (PS);
xi fizička zaštita (PE);
xii oporavak (RE);
xiii upravljanje rizikom (RM);
xiv procjena sigurnosti (CA);
xv informiranost o stanju (SA);
xvi zaštita sustava i komunikacije (SC) i
xvii integritet sustava i informacija (SI).

Razine zrelosti

U okviru modela CMMC upotrebljava se **pet razina zrelosti** definiranih na temelju procesa i praksi. Kako bi postigla određenu razinu zrelosti u CMMC-u, organizacija mora ispuniti preduvjete za postupke i prakse za tu razinu. To podrazumijeva i ispunjavanje preduvjeta za sve razine ispod te razine.

Slika 10. Razine zrelosti u okviru CMMC-a



PROCESSES	PROCESI
Optimizing	Optimizirani
Reviewed	Preispitani
Managed	Upravljani
Documented	Dokumentirani
Performed	Provode
PRACTICES	PRAKSE
Advanced/Progressive	Napredne/progresivne
Proactive	Proaktivne
Good Cyber Hygiene	Dobra kiberhigijena
Intermediate Cyber Hygiene	Srednja kiberhigijena
Basic Cyber Hygiene	Osnovna kiberhigijena
Level 5	5. razina
Level 4	4. razina
Level 3	3. razina
Level 2	2. razina
Level 1	1. razina

- **1. razina**
  - **postupci se provode**: s obzirom na to da organizacija može provoditi te prakse samo na *ad hoc* način i može se, ali ne mora, oslanjati na dokumentaciju. Zrelost postupka ne ocjenjuje se za 1. razinu;
  - **prakse – osnovna kiberhigijena**: prva razina usmjerena je na zaštitu FCI-ja (savezne ugovorne informacije) i sastoji se samo od praksi koje odgovaraju osnovnim zahtjevima u pogledu zaštite;
- **2. razina**
  - **postupci se dokumentiraju**: u 2. razini zahtijeva se da organizacija uspostavi i dokumentira prakse i politike za usmjeravanje provedbe modela CMMC. Dokumentiranje praksi omogućuje pojedincima da ih opetovano provode na isti način. Organizacije razvijaju zrele kapacitete dokumentiranjem svojih procesa i njihovim provođenjem kako je dokumentirano;
  - **prakse – srednja kiberhigijena**: druga razina služi kao prelazak s 1. razine na 3. razinu i sastoji se od podskupa sigurnosnih zahtjeva navedenih u NIST SP 800 – 71 te praksi iz drugih normi i upućivanja;
- **3. razina**
  - **postupcima se upravlja**: u 3. razini zahtijeva se da organizacija uspostavi, održava i financira plan kojim se dokazuje upravljanje aktivnostima za provedbu prakse. Plan može uključivati informacije o nadležnostima, ciljevima, projektnim planovima, resursima, potrebnom osposobljavanju i uključivanju relevantnih dionika;
  - **prakse – dobra kiberhigijena**: treća razina usmjerena je na zaštitu CUI-ja i obuhvaća sve sigurnosne zahtjeve navedene u NIST SP 800 – 171, kao i dodatne prakse iz drugih normi i upućivanja za ublažavanje prijetnji;

- **4. razina**
  - **postupci se preispituju**: u 4. razini zahtijeva se da organizacija preispituje i mjeri prakse u pogledu djelotvornosti. Uz prakse mjerenja djelotvornosti, organizacije na toj razini mogu prema potrebi poduzeti korektivne mjere i redovito obavješćivati više rukovodstvo o statusu ili pitanjima;
  - **prakse – proaktivne**: četvrta razina usmjerena je na zaštitu CUI-ja (kontrolirane neklasificirane informacije) i obuhvaća podskup poboljšanih sigurnosnih zahtjeva. Tim se praksama poboljšava sposobnost organizacije da otkrije i reagira na promjene u taktikama, tehnikama i postupcima te im se prilagođava;
- **5. razina**
  - **postupci se optimiziraju**: u 5. razini od organizacije se zahtijeva da normira i optimizira provedbu postupaka u cijeloj organizaciji;
  - **prakse – napredne/proaktivne**: peta razina usmjerena je na zaštitu CUI-ja. Dodatnim praksama povećava se dubina i sofisticiranost kapaciteta u području kibersigurnosti.

Metoda procjene

CMMC je relativno mladi model koji je dovršen u prvom tromjesečju 2020. Do sada nije bio korišten u okviru nijedne organizacije. Međutim, ugovaratelji Ministarstva obrane očekuju da će se obratiti ovlaštenim ispitivačima treće strane kako bi proveli revizije. Ministarstvo obrane od svojih ugovaratelja očekuje da provode najbolje prakse za poticanje kibersigurnosti i zaštite osjetljivih informacija.

A.6 Model zrelosti kibersigurnosti zajednice (CCSMM)

Model zrelosti kibersigurnosti zajednice (CCSMM) razvio je Centar za osiguranje infrastrukture i sigurnost na Sveučilištu u Teksasu. Cilj je CCSMM-a bolje definirati metode za utvrđivanje postojećeg statusa zajednice u njezinoj kiberpripravnosti i osigurati plan koji zajednice trebaju slijediti u svojim naporima u pogledu pripreme. Zajednice obuhvaćene CCSMM-om uglavnom su lokalne ili državne vlade. Model CCSMM osmišljen je 2007. godine.

Atributi/dimenzije

Razine zrelosti definirane su u skladu sa **šest glavnih dimenzija** koje obuhvaćaju različite aspekte kibersigurnosti unutar zajednica i organizacija. Te su dimenzije jasno definirane za svaku razinu zrelosti (detaljno na slici 11.: Sažetak dimenzija **CCSMM**-a prema razinama) Šest dimenzija navedeno je u nastavku:

i uklonjene prijetnje;
ii parametri;
iii dijeljenje informacija;
iv tehnologija;
v osposobljavanje i
vi test.

Razine zrelosti

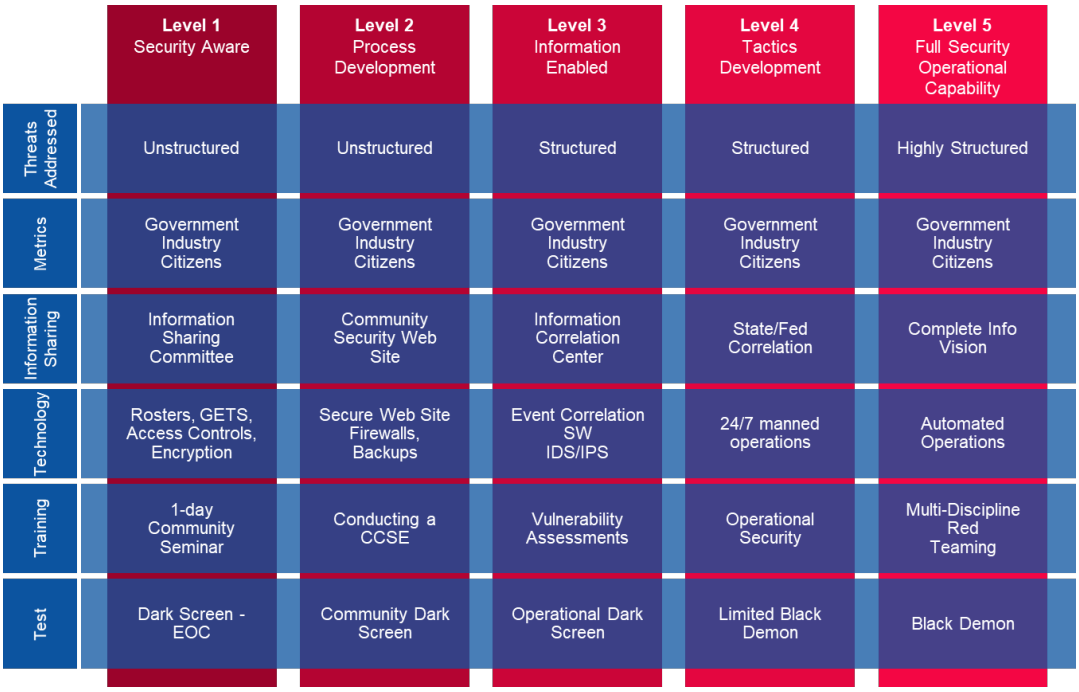
Model CCSMM oslanja se **na pet razina zrelosti** na temelju glavnih vrsta prijetnji i aktivnosti koje se rješavaju na razini:

- **Prva razina: svijest o sigurnosti**
  Glavna tema aktivnosti na ovoj razini jest osvijestiti pojedince i organizacije o prijetnjama, problemima i pitanjima povezanima s kibersigurnošću.
- **Druga razina: razvoj postupka**
  Razina je osmišljena kako bi se zajednicama pomoglo da uspostave i poboljšaju sigurnosne procese potrebne za učinkovito rješavanje pitanja kibersigurnosti.
- **3. razina: omogućivanje informacija**
  Razina je osmišljena s ciljem poboljšanja mehanizama razmjene informacija unutar

zajednice kako bi se zajednici omogućilo da učinkovito poveže naizgled nejednake informacije.

- **4. razina: razvoj taktike**
  Elementi ove razine osmišljeni su kako bi se razvile bolje i proaktivnije metode za otkrivanje napada i odgovor na njih. Do te bi razine trebalo uvesti većinu preventivnih metoda.
- **5. razina: potpuna operativna sposobnost u pogledu sigurnosti**
  Ova razina predstavlja one elemente koji bi trebali biti uspostavljeni kako bi se svaka organizacija smatrala potpuno operativno spremnom za suočavanje s bilo kojom vrstom kiberprijetnji.

Slika 11: Sažetak dimenzija CCSMM-a prema razinama



Level 1	1. razina
Security Aware	svijest o sigurnosti
Level 2	2. razina
Process Development	razvoj postupka
Level 3	3. razina
Information Enabled	omogućivanje informacija
Level 4	4. razina
Tactics Development	razvoj taktike
Level 5	5. razina
Full Security Operational Capability	potpuna operativna sposobnost u pogledu sigurnosti
Threats Addressed	uklonjene prijetnje
Metrics	parametri
Information sharing	razmjena informacija
Technology	tehnologija
Training	osposobljavanje
Test	test
Unstructured	nestrukturirano
Governement	vlada
Industry	industrija
Citizens	građani
Information Sharing Committee	Odbor za razmjenu informacija
Rosters, GETS, Assess Controls, Encryption	popisi, GETS, kontrole pristupa, šifriranje
1-dat Community Seminar	jednodnevni seminar zajednice
Dark Screen – EOC	vježba Dark screen – EOC
Unstructured	nestrukturirano
Governement	vlada
Industry	industrija
Citizens	građani
Community Security Web site	mrežno mjesto za sigurnost zajednice
Secure Web Site Firewalls, Backups	sigurni vatrozidovi i sigurnosne kopije mrežnih mjesta
Conudcting a CCSE	provedba postupka CCSE

Community Dark Screen	vježba Dark screen usmjerena na zajednicu
Structured	strukturirano
Governement	vlada
Industry	industrija
Citizens	građani
Information Correlation Center	Podatkovni korelacijski centar
Event Correlation SW IDS/IPS	korelacija događaja SW IDS/IPS
Vulnerability Assessment	procjena osjetljivosti
Operational Dark Screen	vježba Dark screen usmjerena na operativne aspekte
Structured	strukturirano
Governement	vlada
Industry	industrija
Citizens	građani
State/Fed Correlation	korelacija na razini države / savezna korelacija
24/7 manned operations	operacije koje uključuju osoblje 24 sata dnevno sedam dana u tjednu
Operational Security	operativna sigurnost
Limited Black Demon	ograničeni Black Demon
Highly Structured	vrlo strukturirano
Complete Info	vizija potpunosti
Vision	informacija
Automated	automatizirane
Operations	operacije
Multi-Discipline	višedisciplinarni
Red	Red
Teaming	Teaming
Black Demon	Black Demon

Metoda procjene

Cilj je CCSMM-a kao metodologije procjene da se uvede u zajednicama uz doprinos državnih i saveznih agencija za izvršavanje zakonodavstva. Njime se nastoji pomoći zajednici da definira što je najvažnije, koji su najvjerojatniji ciljevi i što treba zaštititi (i u kojoj mjeri). Imajući na umu te ciljeve, mogu se izraditi planovi kako bi se svaki aspekt zajednice doveo do potrebne razine zrelosti kibersigurnosti. Posebni podatci dobiveni u okviru CCSMM-a pomažu u definiranju ciljeva različitih ispitivanja i vježbi koje se mogu upotrijebiti za mjerenje djelotvornosti uspostavljenih programa.

A.7 Model zrelosti informacijske sigurnosti za okvir kibersigurnosti NIST-a (ISMM)

Model zrelosti informacijske sigurnosti (ISMM) razvijen je u okviru Koledža za računalne znanosti i inženjerstvo pri Sveučilištu nafte i minerala „Kralj Fahd” u Saudijskoj Arabiji. U njemu se predlaže novi model zrelosti kapaciteta za mjerenje provedbe mjera u području kibersigurnosti. Cilj je ISMM-a omogućiti organizacijama da redovito mjere svoj napredak u provedbi primjenom istog alata za mjerenje kako bi se osiguralo održavanje željenog položaja u pogledu sigurnosti. ISMM je razvijen 2017.

Atributi/dimenzije

ISMM se temelji na postojećim procijenjenim područjima okvira NIST-a i dodaje dimenziju procjene usklađenosti. Time se model povećava na **23 ocijenjena područja** za položaj organizacije u pogledu sigurnosti. U nastavku se navode 23 ocijenjena područja:

i upravljanje imovinom;
ii poslovno okruženje;
iii upravljanje;
iv procjena rizika;
v strategija upravljanja rizicima;
vi procjena sukladnosti;
vii kontrola pristupa;
viii informiranost i osposobljavanje;
ix sigurnost podataka
x procesi i postupci za zaštitu informacija;
xi održavanje;
xii zaštitna tehnologija;
xiii neuobičajene aktivnosti i događaji;

xiv kontinuirano praćenje sigurnosti;
xv postupci otkrivanja;
xvi planiranje odgovora;
xvii komunikacija o odgovoru;
xviii analiza odgovora;
xix ublažavanje odgovora;
xx poboljšanje odgovora;
xxi planiranje oporavka;
xxii poboljšanje oporavka i
xxiii komunikacija o oporavku.

Razine zrelosti

ISMM se oslanja na **pet razina zrelosti** koje nažalost nisu detaljno opisane u dostupnoj dokumentaciji.

- **1. razina:** postupak je proveden;
- **2. razina:** postupkom se upravlja;
- **3. razina** postupak je uspostavljen;
- **4. razina** postupak je predvidljiv;
- **5. razina** postupak se optimizira.

Metoda procjene

U okviru ISMM-a ne predlaže se nikakva posebna metodologija za provedbu procjene za organizacije.

A.8 Model sposobnosti unutarnje revizije (IA-CM) za javni sektor

Model sposobnosti unutarnje revizije (IA-CM) razvila je Zaklada za istraživanje Instituta unutarnjih revizora u cilju izgradnje kapaciteta i zastupanja interesa putem samoprocjene u javnom sektoru. Model IA-CM namijenjen je stručnjacima za reviziju te pruža pregled samog modela zajedno s Vodičem za primjenu kako bi se pomoglo u primjeni modela kao alata za samoprocjenu.

Unatoč tome što je IA-CM usredotočen na sposobnost unutarnje revizije, a ne na izgradnju kapaciteta u području kibersigurnosti, model je osmišljen kao alat za samoprocjenu za subjekte javnog sektora koji se može primijeniti na globalnoj razini kako bi se poboljšali postupci i djelotvornost. Budući da njegov opseg nije usmjeren na kibersigurnost, atributi se neće analizirati. Model IA-CM dovršen je 2009. godine.

Razine zrelosti

Model sposobnosti unutarnje revizije (IA-CM) obuhvaća **pet razina zrelosti**, od kojih svaka opisuje značajke i sposobnosti aktivnosti unutarnje revizije na toj razini. Razine sposobnosti u modelu sadržavaju plan za kontinuirano poboljšavanje.

- **1. razina: Početak**
  nema održivih, ponovljivih sposobnosti – ovisi o pojedinačnim naporima
  - *ad hoc* ili nestrukturirano.
  - pojedinačne revizije ili preispitivanja dokumenata i transakcija radi točnosti i usklađenosti
  - rezultati ovise o vještinama određene osobe koja obavlja tu zadaću
  - nema drugih profesionalnih praksi osim onih koje osiguravaju strukovna udruženja
  - prema potrebi, odobrenje za financiranje koje daje uprava
  - nepostojanje infrastrukture
  - revizori vjerojatno čine dio veće organizacijske jedinice
  - institucijski kapaciteti nisu razvijeni
- **2. razina: Infrastruktura**
  održive i ponovljive prakse i postupci
  - ključno pitanje ili izazov u pogledu 2. razine jest kako uspostaviti i održati ponovljivost procesa, a time i sposobnost ponovljivosti

- uspostavljaju se odnosi izvješćivanja o unutarnjoj reviziji, upravljačka i administrativna infrastruktura te stručne prakse i postupci (smjernice, procesi i postupci unutarnje revizije)
- planiranje revizija koje se uglavnom temelji na prioritetima upravljanja
- trajno oslanjanje uglavnom na vještine i kompetencije određenih osoba
- djelomična sukladnost s normama

▶ **3. razina: Integracija**
prakse upravljanja i profesionalne prakse ujednačeno se primjenjuju
- politike, procesi i postupci unutarnje revizije definiraju se, dokumentiraju i integriraju u infrastrukturu organizacije
- upravljanje unutarnjim revizijama i stručne prakse dobro su uhodani i ujednačeno se primjenjuju u okviru aktivnosti unutarnje revizije
- unutarnja revizija počinje se usklađivati s poslovanjem organizacije i rizicima s kojima se suočava
- unutarnja revizija razvija se od provođenja isključivo tradicionalne unutarnje revizije do integracije u timski rad te pružanja savjeta o uspješnosti i upravljanju rizicima
- naglasak je na izgradnji tima i kapacitetu aktivnosti unutarnje revizije te njezinoj neovisnosti i objektivnosti
- općenito je u skladu s normama.

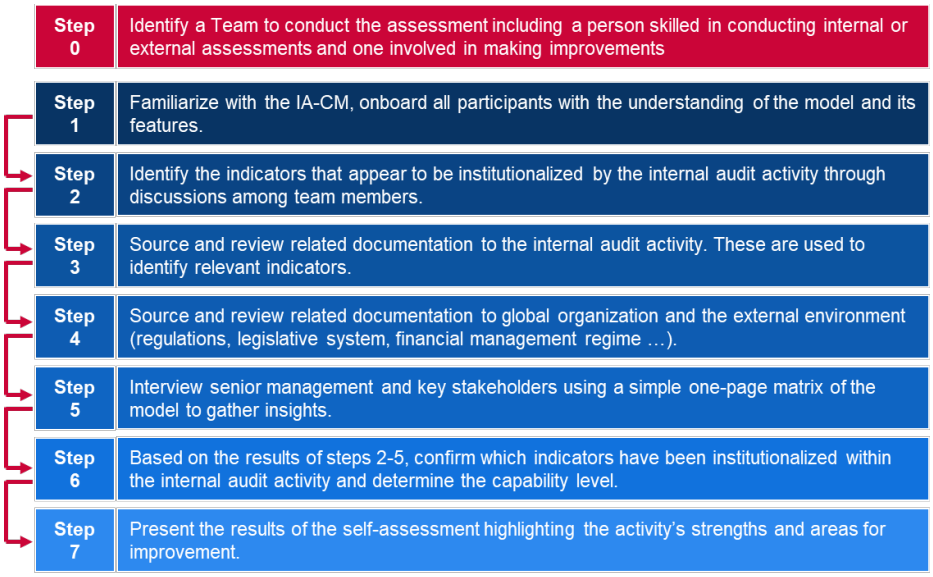
▶ **4. razina: Upravljanje**
objedinjuju se informacije iz cijele organizacije kako bi se poboljšalo upravljanje i upravljanje rizicima
- unutarnja revizija i očekivanja ključnih dionika usklađeni su
- uspostavljeni su parametri uspješnosti za mjerenje i praćenje postupaka i rezultata unutarnje revizije
- smatra se da unutarnja revizija organizaciji daje znatan doprinos
- funkcija unutarnje revizije sastavni je dio upravljanja i upravljanja rizicima organizacije
- unutarnja revizija poslovna je sastavnica kojom se dobro upravlja
- rizici se kvantitativno mjere i njima se upravlja kvantitativno
- uspostavljene su potrebne vještine i kompetencije s kapacitetom za obnovu i razmjenu znanja (unutarnjom revizijom i u cijeloj organizaciji)

▶ **5. razina: Optimizacija**
učenje unutar i izvan organizacije radi stalnog poboljšanja
- unutarnja revizija organizacija je za učenje s trajnim poboljšanjima procesa i inovacijama
- u unutarnjoj reviziji upotrebljavaju se informacije iz unutar i izvan organizacije kako bi se pridonijelo postizanju strateških ciljeva
- vrhunska/preporučena/najbolja praksa
- unutarnja revizija ključan je dio upravljačke strukture organizacije
- vrhunske stručne i specijalizirane vještine
- pojedinačne, jedinične i organizacijske mjere učinkovitosti u potpunosti su integrirane radi
- poticanja poboljšanja učinkovitosti

Metoda procjene

Model sposobnosti unutarnje revizije (IA-CM) jasno je izrađen za samoprocjenu. Sadržava detaljne korake koje treba slijediti pri upotrebi IA-CM-a i prezentacijske uzorke za prilagodbu. Prije početka samoprocjene potrebno je odrediti poseban tim, uključujući najmanje jednu osobu koja posjeduje vještine za provođenje unutarnjih ili vanjskih procjena unutarnjih revizija i jednu osobu koja sudjeluje u poboljšanjima u tom području.

Slika 12.: Koraci samoprocjene u modelu IC-AM



Step 0	0. korak
Step 1	1. korak
Step 2	2. korak
Step 3	3. korak
Step 4	4. korak
Step 5	5. korak
Step 6	6. korak
Step 7	7. korak
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	određivanje tima za provedbu procjene, uključujući osobu koja posjeduje vještine za provođenje unutarnjih ili vanjskih procjena i osobu koja sudjeluje u poboljšanjima
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	upoznavanje s modelom IA-CM, svi sudionici trebaju razumjeti model i njegove značajke
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	utvrđivanje pokazatelja za koje se čini da su institucionalizirani u okviru aktivnosti unutarnje revizije održavanjem rasprave među članovima tima
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	prikupljanje i pregled dokumentacije povezane s aktivnostima unutarnje revizije upotrebljavaju se za utvrđivanje relevantnih pokazatelja
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	prikupljanje i pregled dokumentacije povezane s globalnom organizacijom i vanjskim okruženjem (uredbe, zakonodavni sustav, sustav financijskog upravljanja...)
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	razgovor s višim rukovodstvom i ključnim dionicima s pomoću jednostavne matrice modela od jedne stranice kako bi se prikupile spoznaje
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	na temelju rezultata koraka 2. – 5., potvrđivanje koji su pokazatelji institucionalizirani u okviru aktivnosti unutarnje revizije i određivanje razine kapaciteta
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	predstavljanje rezultata samoprocjene s naglaskom na prednostima aktivnosti i područjima u kojima su potrebna poboljšanja

A.9 Globalni indeks kibersigurnosti (GCI)

Globalni indeks kibersigurnosti (GCI) inicijativa je Međunarodne unije za telekomunikacije (ITU) čiji je cilj preispitivanje predanosti kibersigurnosti i situacije u svim regijama ITU-a: Africi, Sjevernoj i Južnoj Americi, arapskim državama, azijsko-pacifičkoj regiji, Zajednici neovisnih država (ZND) i Europi te u središte pozornosti stavlja zemlje s velikom predanošću i preporučljivim praksama. Cilj je GCI-ja pomoći zemljama u utvrđivanju područja u kojima su potrebna poboljšanja u pogledu kibersigurnosti te ih motivirati da poduzmu mjere za poboljšanje poretka, čime će se pridonijeti podizanju opće razine kibersigurnosti diljem svijeta.

S obzirom na to da je GCI indeks, a ne model zrelosti, ne koristi se razinama zrelosti, nego ocjenom za rangiranje i usporedbu globalne obveze država i regija u području kibersigurnosti.

Atributi/dimenzije

Globalni indeks kibersigurnosti (GCI) temelji se na pet stupova Globalnog programa za kibersigurnost (GCA). Ti stupovi čine pet podindeksa GCI-ja i svaki uključuje skup pokazatelja. Pet stupova i pokazatelja navedeno je u nastavku:

i **Pravni okvir**: mjere se temelje na postojanju pravnih institucija i okvira koji se bave kibersigurnošću i kiberkriminalitetom.
- Zakonodavstvo u području kiberkriminaliteta
- propisi o kibersigurnosti i
- ograničavanje zakonodavstva o neželjenoj pošti.

ii **Tehnički stup**: mjere se temelje na postojanju tehničkih institucija i okvira koji se bave kibersigurnošću.
- CERT/CIRT/CSRIT;
- okvir za provedbu normi;
- tijelo za normizaciju;
- tehnički mehanizmi i sposobnosti uvedene za rješavanje problema neželjene pošte;
- korištenje oblaka za potrebe kibersigurnosti i
- mehanizmi za zaštitu djece na internetu.

iii **Organizacijski stup**: mjere se temelje na postojanju institucija za koordinaciju politika i strategija za razvoj kibersigurnosti na nacionalnoj razini.
- nacionalna strategija za kibersigurnost;
- nadležna agencija i
- kibersigurnost.

iv **Izgradnja kapaciteta**: mjere koje se temelje na programima istraživanja i razvoja, obrazovanju i osposobljavanju, certificiranim stručnjacima i agencijama javnog sektora kojima se potiče izgradnja kapaciteta.
- kampanje za osvješćivanje javnosti;
- okvir za certifikaciju i akreditaciju stručnjaka za kibersigurnost;
- tečajevi stručnog osposobljavanja u području kibersigurnosti;
- obrazovni ili akademski programi u području kibersigurnosti;
- programi istraživanja i razvoja u području kibersigurnosti i
- mehanizmi poticaja.

v **Suradnja**: mjere koje se temelje na partnerstvima, okvirima suradnje i mrežama za razmjenu informacija.
- Bilateralni sporazumi;
- multilateralni sporazumi;
- sudjelovanje u međunarodnim forumima/udruženjima;
- javno-privatna partnerstva;
- međuagencijska partnerstva / partnerstva unutar agencije i
- primjeri najbolje prakse.

Metoda procjene

GCI je alat za samoprocjenu izrađen istraživanjem[30] binarnih, unaprijed kodiranih i otvorenih pitanja. Upotrebom binarnih odgovora uklanja se procjena na temelju mišljenja i moguća pristranost prema određenim vrstama odgovora. Unaprijed kodiranim odgovorima štedi se vrijeme i omogućuje točnija analiza podataka. Osim toga, jednostavan dihotomski raspon omogućuje brže i složenije ocjenjivanje jer za to nisu potrebni opsežni odgovori, čime se ubrzava i pojednostavnjuje postupak odgovaranja i daljnje ocjene. Ispitanik samo treba potvrditi postojanje ili nepostojanje određenih prethodno utvrđenih rješenja za kibersigurnost. Internetski mehanizam istraživanja, koji se upotrebljava za prikupljanje odgovora i učitavanje relevantnih materijala, omogućuje skupini stručnjaka da izdvoje primjere dobre prakse i skup tematskih kvalitativnih procjena.

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

Cjelokupni proces GCI-ja provodi se kako slijedi:

- svim sudionicima šalje se pozivno pismo u kojem ih se obavješćuje o inicijativi i traži se točka za kontakt odgovorna za prikupljanje svih relevantnih podataka i ispunjavanje internetskog upitnika za GCI. Tijekom internetske ankete ITU službeno poziva odobrenu središnju točku za kontakt da odgovori na upitnik;
- prikupljanje primarnih podataka (za zemlje koje ne ispunjavaju upitnik):
  - ITU razrađuje početni nacrt odgovora na upitnik koristeći se javno dostupnim podatcima i istraživanjem na internetu;
  - nacrt upitnika šalje se središnjim točkama za kontakt na pregled;
  - središnje točke za kontakt poboljšavaju točnost i zatim vraćaju nacrt upitnika;
  - ispravljeni nacrt upitnika šalje se svakoj središnjoj točki za kontakt na konačno odobrenje i
  - validirani upitnik koristi se za analizu, ocjenjivanje i rangiranje.
- sekundarno prikupljanje podataka (za zemlje koje odgovaraju na upitnik):
  - ITU utvrđuje sve odgovore koji nedostaju, popratne dokumente, poveznice itd.;
  - središnja točka za kontakt po potrebi poboljšava točnost odgovora;
  - ispravljeni nacrt upitnika šalje se svakoj središnjoj točki za kontakt na konačno odobrenje i
  - validirani upitnik koristi se za analizu, ocjenjivanje i rangiranje.

A.10 Indeks kibersposobnosti (CPI)

Indeks kibersposobnosti (CPI) osmislio je istraživački program jedinice Economist Intelligence Unit pod pokroviteljstvom poduzeća Booz Allen Hamilton 2011. CPI je „dinamički kvantitativni i kvalitativni model [...] kojim se mjere posebne značajke kiberprostora u okviru četiriju pokretača kibersposobnosti: pravni i regulatorni okvir, gospodarski i socijalni kontekst, tehnološka infrastruktura i primjena u industriji te se proučava digitalni napredak u četirima ključnim industrijama”.[31] Cilj je CPI-ja usporediti sposobnost zemalja skupine G20 da se odupru kibernapadima i uvedu potrebnu digitalnu infrastrukturu za uspješno i sigurno gospodarstvo. Referentna vrijednost CPI-ja usmjerena je na 19 zemalja skupine G20 (isključujući EU). Indeksom se zatim određuje poredak zemalja za svaki pokazatelj.

Atributi/dimenzije

Indeks kibersposobnosti (CPI) temelji se na četirima pokretačima kibersposobnosti. Svaka se kategorija zatim mjeri s pomoću više pokazatelja kako bi se svakoj zemlji dodijelila posebna ocjena. Kategorije i stupovi navedeni su u nastavku:

i **Pravni i regulatorni okvir**
- predanost vlade razvoju kibersigurnosti
- politike u području kiberzaštite
- kibercenzura (ili nepostojanje kibercenzure)
- politička učinkovitost
- zaštita intelektualnog vlasništva

ii **Gospodarski i socijalni kontekst**
- Razina obrazovanja
- tehničke vještine
- otvorenost trgovine
- stupanj inovativnosti u poslovnom okruženju

iii **Tehnološka infrastruktura**
- pristup informacijskoj i komunikacijskoj tehnologiji
- kvaliteta informacijske i komunikacijske tehnologije
- cjenovna pristupačnost informacijske i komunikacijske tehnologije
- rashodi za informacijsku tehnologiju
- broj sigurnih poslužitelja

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

iv **Primjena u industriji**
- pametne mreže
- e-zdravstvo
- e-trgovina
- inteligentni prijevoz
- e-vlada

Metoda procjene

CPI je kvantitativni i kvalitativni model ocjenjivanja. Procjenu je provela jedinica Economist Intelligence Unit upotrebom kvantitativnih pokazatelja iz dostupnih statističkih izvora i procjenama u slučaju nedostatka podataka. Glavni su korišteni izvori jedinica Economist Intelligence Unit, Organizacija UN-a za obrazovanje, znanost i kulturu (UNESCO), Međunarodna telekomunikacijska unija (ITU) i Svjetska banka.

A.11 Indeks kibersposobnosti (CPI)

U ovom su odjeljku sažeti glavni nalazi analize postojećih modela zrelosti. Tablica 5.: Pregled analiziranih modela zrelosti daje pregled glavnih značajki svakog modela u skladu s izmijenjenim Beckerovim modelom. U tablici 6. Usporedba razina zrelosti analiziranih modela na visokoj razini. Tablica 7. daje pregled dimenzija ili atributa koji se upotrebljavaju u svakom modelu.

Tablica 5.: Pregled analiziranih modela zrelosti

Naziv modela	Institucija koja je služila kao izvor	Svrha	Cilj	Broj razina	Broj atributa	Metoda procjene	Prikaz rezultata
Model zrelosti kapaciteta u području kibersigurnosti za države (CMM)	Globalni centar za kapacitete u području kibersigurnosti Sveučilište u Oxfordu	Povećati opseg i djelotvornost izgradnje kapaciteta u području kibersigurnosti na međunarodnoj razini	Zemlje	5	5 glavnih dimenzija	Suradnja s lokalnim organizacijama kako bi se model prilagodio prije njegove primjene u nacionalnom kontekstu	Radar pet odjeljaka
Model zrelosti kapaciteta u području kibersigurnosti (C2M2)	Ministarstvo energetike SAD-a (DOE)	Pomoći organizacijama da evaluiraju i poboljšaju svoje programe u području kibersigurnosti i ojačaju svoju operativnu otpornost	Organizacije svih sektora, vrsta i veličina	4	10 glavnih domena	Metodologija i skup alata za samoocjenjivanje	Kartica za ocjenjivanje s tortnim grafikonima
Okvir za poboljšanje kibersigurnosti ključne infrastrukture	Nacionalni institut za norme i tehnologiju (NIST)	Okvir za usmjeravanje aktivnosti i upravljanje rizicima unutar organizacija u području kibersigurnosti	Organizacije	Nije primjenjivo (4 reda)	5 osnovnih funkcija	Samoprocjena	-
Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2)	Pravni fakultet Sveučilišta u Kataru	Izvediv model koji se može upotrijebiti za utvrđivanje, mjerenje i razvoj okvira za kibersigurnost Katara	Katarske organizacije	5	5 glavnih domena	–	-
Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)	Ministarstvo obrane SAD-a (DOD)	Poticanje najboljih praksi u području kibersigurnosti radi zaštite informacija	Organizacije sektora industrije i obrane (DIB)	5	17 glavnih domena	Procjena koju provode revizori treće strane	-
Model zrelosti kibersigurnosti zajednice (CCSMM)	Centar za osiguranje infrastrukture i sigurnost pri Sveučilištu u Teksasu	Utvrđivanje postojećeg statusa zajednice u njezinoj kiberpripravnosti i osiguranje plana koji zajednice trebaju slijediti u svojim naporima u pogledu pripreme	Zajednice (lokalne ili državne vlade)	5	6 glavnih dimenzija	Procjena unutar zajednica uz doprinos državnih i saveznih agencija za izvršavanje zakonodavstva	-
Model zrelosti informacijske sigurnosti za okvir kibersigurnosti NIST-a (ISMM)	Visoka škola za informatiku i inženjerstvo Sveučilište nafte i minerala „Kralj Fahd” Dhahran, Saudijska Arabija	Omogućivanje organizacijama da mjere svoj napredak u provedbi tijekom vremena kako bi se osiguralo da održavaju željeni položaj u pogledu sigurnosti	Organizacije	5	23 ocijenjena područja	–	-
Model sposobnosti unutarnje revizije (IA-CM) za javni sektor	Zaklada za istraživanje Instituta unutarnjih revizora	Izgradnja kapaciteta unutarnje revizije i zastupanja interesa s pomoću samoprocjene u javnom sektoru	Organizacije javnog sektora	5	6 elemenata	Samoprocjena	-
Globalni indeks kibersigurnosti (GCI)	Međunarodna unija za telekomunikacije (ITU)	Preispitati predanost i stanje u području kibersigurnosti te pomoći zemljama u utvrđivanju područja u kojima su potrebna poboljšanja kad je riječ o kibersigurnosti	Zemlje	NIJE PRIMJENJIVO	5 stupova	Samoprocjena	Rang-lista

Indeks kibersposobnosti (CPI)	Jedinica Economist Intelligence Unit i poduzeće Booz Allen Hamilton	Uspoređivanje kapaciteta zemalja skupine G20 da se odupru kibernapadima i uvedu potrebnu digitalnu infrastrukturu za uspješno i sigurno gospodarstvo.	Zemlje skupine G20	NIJE PRIMJENJIVO	4 kategorije	Komparativna analiza koju provodi jedinica Economist Intelligence Unit	Rang-lista

Tablica 6 Usporedba razina zrelosti

Model	1. razina	2. razina	3. razina	4. razina	5. razina
Model zrelosti kapaciteta u području kibersigurnosti za države (CMM)	**Početak** Ne postoji zrelost kibersigurnosti ili je tek u začetku. Možda će se održati početne rasprave o izgradnji kapaciteta u području kibersigurnosti, ali nisu poduzete konkretne mjere. U ovoj fazi nema vidljivih dokaza.	**Razvoj** Neke značajke aspekata počele su rasti i formuliraju se, ali mogu biti *ad hoc*, neorganizirane, loše definirane ili jednostavno „nove”. Međutim, dokazi o toj aktivnosti mogu se jasno predstaviti.	**Utvrđivanje** elementi tog aspekta uspostavljeni su i funkcioniraju. Međutim, ne postoji dobro promišljeno razmatranje relativne raspodjele sredstava. U pogledu „relativnih” ulaganja u različite elemente tog aspekta donesen je mali broj kompromisnih odluka. Međutim, taj je aspekt funkcionalan i definiran.	**Strategija** donesene su odluke o tome koji su dijelovi aspekta važni i koji su manje važni za određenu organizaciju ili državu. Strateška faza odražava činjenicu da su ti izbori doneseni ovisno o okolnostima države ili organizacije.	**Dinamičnost** Postoje jasni mehanizmi za izmjenu strategije ovisno o prevladavajućim okolnostima kao što su tehnologija okruženja prijetnji, globalni sukob ili značajna promjena u jednom problematičnom području (npr. kiberkriminalitet ili privatnost). Dinamične organizacije razvile su napredne metode za promjenu strategija. Ova faza odlikuje se brzim donošenjem odluka, preraspodjelom resursa i stalnom pozornošću koja se posvećuje okruženju koje se mijenja.
Model zrelosti kapaciteta u području kibersigurnosti (C2M2)	**0. razina zrelosti pokazatelja (MIL0)** Prakse se ne provode.	**1. razina zrelosti pokazatelja (MIL1)** Početne se prakse provode, ali mogu biti *ad hoc*.	**2. razina zrelosti pokazatelja (MIL2)** Značajke upravljanja: prakse se dokumentiraju; osigurani su odgovarajući resursi za potporu procesu; osoblje koje provodi prakse posjeduje odgovarajuće vještine i znanje i dodijeljene su odgovornosti i ovlasti za provedbu prakse. Značajka pristupa: prakse su potpunije ili naprednije nego na 1. razini zrelosti pokazatelja.	**3. razina zrelosti pokazatelja (MIL3)** Značajke upravljanja: aktivnosti se vode politikama (ili drugim organizacijskim direktivama); Ciljevi uspješnosti za aktivnosti u okviru domene utvrđeni su i prate se kako bi se pratila postignuća i dokumentirane prakse za aktivnosti u okviru domene normirane su i poboljšane u cijelom poduzeću. Značajka pristupa: prakse su potpunije ili naprednije nego na 2. razini zrelosti pokazatelja.	–
Model zrelosti informacijske sigurnosti za okvir	**Postupak se provodi**	**Postupkom se upravlja**	**Postupak je uspostavljen**	**Postupak je predvidljiv**	**Postupak se optimizira**

kibersigurnosti NIST-a (ISMM)					
Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2)	**Početak** Primjenjuju se *ad hoc* prakse i postupci u pogledu kibersigurnosti u nekim područjima.	**Razvoj** Provedene politike i prakse za razvoj i poboljšanje kibersigurnosnih aktivnosti u okviru domena s ciljem predlaganja novih aktivnosti koje treba provesti.	**Provedba** Donesene politike za provedbu svih kibersigurnosnih aktivnosti u okviru domena s ciljem dovršetka provedbe u određenom trenutku.	**Prilagodljivost** Pregledavaju se i preispituju aktivnosti u području kibersigurnosti te usvajaju prakse na temelju prediktivnih pokazatelja koji proizlaze iz prethodnih iskustava i mjera.	**Brzina** Nastavlja se s prilagodljivom fazom s dodatnim naglaskom na brzini pri provedbi aktivnosti u tim područjima.
Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)	**Postupci: izvršeni** Budući da organizacija može provoditi te prakse samo na *ad hoc* način i može se, ali ne mora oslanjati na postupak dokumentiranja, ne ocjenjuje se zrelost postupka dokumentiranja za razinu 1. **Prakse:** osnovna kiberhigijena Prva razina usmjerena je na zaštitu saveznih ugovornih informacija (FCI) i sastoji se samo od praksi koje odgovaraju osnovnim zahtjevima u pogledu zaštite.	**Postupci: dokumentirani** U 2. razini zahtijeva se da organizacija uspostavi i dokumentira prakse i politike za usmjeravanje provedbe modela CMMC. Dokumentiranje praksi omogućuje pojedincima da ih provode na ponovljiv način. Organizacije razvijaju zrele kapacitete dokumentiranjem svojih procesa i njihovim kasnijim provođenjem kako je dokumentirano. **Prakse: srednja kiberhigijena** Druga razina služi kao prelazak s 1. razine na 3. razinu i sastoji se od podskupa sigurnosnih zahtjeva navedenih u NIST SP 800 – 171 te praksi iz drugih normi i upućivanja.	**Postupci: upravljani** U 3. razini zahtijeva se da organizacija uspostavi, održava i financira plan kojim se dokazuje upravljanje aktivnostima za provedbu prakse. Plan može uključivati informacije o nadležnostima, ciljevima, projektnim planovima, resursima, potrebnom osposobljavanju i uključivanju relevantnih dionika. **Prakse: dobra kiberhigijena** Treća razina usmjerena je na zaštitu kontroliranih neklasificiranih informacija (CUI) i obuhvaća sve sigurnosne zahtjeve navedene u NIST SP 800 – 171, kao i dodatne prakse iz drugih normi i upućivanja za ublažavanje prijetnji.	**Postupci: pregledani** U 4. razini zahtijeva se da organizacija preispituje i mjeri prakse u pogledu djelotvornosti. Uz prakse mjerenja djelotvornosti, organizacije na toj razini mogu prema potrebi poduzeti korektivne mjere i redovito obavješćivati više rukovodstvo o statusu ili pitanjima. **Prakse: proaktivne** Četvrta razina usmjerena je na zaštitu CUI-ja (kontrolirane neklasificirane informacije) i obuhvaća podskup poboljšanih sigurnosnih zahtjeva. Tim se praksama poboljšava sposobnost organizacije da otkrije i odgovori na promjene u taktikama, tehnikama i postupcima te im se prilagođava.	**Postupci: optimizirani** Peta razina zahtijeva od organizacije da normira i optimizira provedbu postupaka u cijeloj organizaciji. **Prakse: Napredne/proaktivne** Peta razina usmjerena je na zaštitu CUI-ja (kontrolirane neklasificirane informacije). Dodatnim praksama povećava se dubina i sofisticiranost kapaciteta u području kibersigurnosti.
Model zrelosti kibersigurnosti zajednice (CCSMM)	**Svijest o sigurnosti** Glavna tema aktivnosti na ovoj razini jest osvijestiti pojedince i organizacije o prijetnjama, problemima i pitanjima povezanima s kibersigurnošću.	**Razvoj procesa** Razina osmišljena kako bi se zajednicama pomoglo da uspostave i poboljšaju sigurnosne procese potrebne za učinkovito rješavanje pitanja kibersigurnosti.	**Omogućene su informacije** Svrha je poboljšati mehanizme razmjene informacija unutar zajednice kako bi se zajednici omogućilo učinkovito povezivanje naizgled nejednakih informacija.	**Razvoj taktike** Elementi ove razine osmišljeni su kako bi se razvile bolje i proaktivnije metode za otkrivanje napada i odgovor na njih. Do te bi razine trebalo uvesti većinu preventivnih metoda.	**Potpuna operativna sposobnost u pogledu sigurnosti** Ova razina predstavlja one elemente koji bi trebali biti uspostavljeni kako bi se svaka organizacija mogla smatrati potpuno operativno spremnom za suočavanje s bilo kojom vrstom kiberprijetnje.
Model sposobnosti unutarnje revizije (IA-CM) za javni sektor	**Početak** Nema održivih, ponovljivih kapaciteta – ovisi o pojedinačnim naporima	**Infrastruktura** Održive i ponovljive prakse i postupci	**Integrirano** Prakse upravljanja i profesionalne prakse ujednačeno se primjenjuju	**Upravljanje** Objedinjuje informacije iz cijele organizacije kako bi se poboljšalo upravljanje i upravljanje rizicima	**Optimizacija** Učenje unutar i izvan organizacije radi stalnog poboljšanja

Tablica 7.: Usporedba atributa/dimenzija

	Model zrelosti kapaciteta u području kibersigurnosti za države (CMM)	Model zrelosti kapaciteta u području kibersigurnosti (C2M2)	Katarski model zrelosti kapaciteta u području kibersigurnosti (Q-C2M2)	Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)	Certifikacija modela zrelosti kapaciteta u području kibersigurnosti (CMMC)	Model zrelosti informacijske sigurnosti za okvir kibersigurnosti NIST-a (ISMM)	Okvir za poboljšanje kibersigurnosti ključne infrastrukture	Globalni indeks kibersigurnosti (GCI)	Indeks kibersposobnosti (CPI)
Razine	Pet dimenzija podijeljeno na nekoliko čimbenika, uključujući višestruke aspekte i pokazatelje (Slika 4.)	Deset domena, jedinstveni cilj upravljanja i nekoliko ciljeva pristupa (Slika 6.)	Pet domena podijeljeno u poddomene	Sedamnaest domena detaljno je razrađeno u procese i jedan ili više kapaciteta koje su zatim podijeljene u prakse (Slika 9.)	Šest glavnih dimenzija	Dvadeset tri ocijenjena područja	Pet funkcija s ključnim kategorijama i potkategorijama (Slika 8.).	Pet stupova, uključujući nekoliko pokazatelja	Četiri kategorije s nekoliko pokazatelja
Atributi/dimenzije	i osmišljavanje politike i strategije u području kibersigurnosti; ii poticanje odgovorne kulture kibersigurnosti u društvu; iii razvoj znanja o kibersigurnosti; iv stvaranje djelotvornih pravnih i regulatornih okvira; v kontroliranje rizika s pomoću normi, organizacija i tehnologija	i upravljanje rizicima; ii upravljanje imovinom, promjenama i konfiguracijom; iii upravljanje identitetom i pristupom; iv upravljanje prijetnjama i ranjivošću; v informiranost o stanju; vi odgovor na događaje i incidente; vii upravljanje lancem opskrbe i vanjskim ovisnostima; viii upravljanje radnom snagom; ix arhitektura kibersigurnosti; x upravljanje programom kibersigurnosti	i razumijevanje (kiberupravljanje, imovina, rizici i osposobljavanje); ii sigurnost (sigurnost podataka, sigurnost tehnologije, sigurnost pristupa, sigurnost komunikacije i sigurnost osoblja); iii izlaganje (praćenje, upravljanje incidentima, otkrivanje, analiza i izloženost); iv odgovor (planiranje odgovora, ublažavanje i komunikacija odgovora); v održavanje (planiranje oporavka, upravljanje kontinuitetom, poboljšanje i vanjske ovisnosti)	i kontrola pristupa; ii upravljanje imovinom; iii revizija i odgovornost; iv informiranost i osposobljavanje; v upravljanje konfiguracijom; vi identifikacija i autentifikacija; vii odgovor na incidente; viii održavanje; ix zaštita medija; x sigurnost osoblja; xi fizička zaštita; xii oporavak; xiii upravljanje rizicima; xiv procjena sigurnosti; xv informiranost o stanju; xvi zaštita sustava i komunikacije; xvii integritet sustava i informacija	i uklonjene prijetnje; ii parametri; iii dijeljenje informacija; iv tehnologija; v osposobljavanje; vi test	i upravljanje imovinom; ii poslovno okruženje; iii upravljanje; iv procjena rizika; v strategija upravljanja rizicima; vi procjena sukladnosti; vii kontrola pristupa; viii informiranost i osposobljavanje; ix sigurnost podataka; x procesi i postupci za zaštitu informacija; xi održavanje; xii zaštitna tehnologija; xiii neuobičajene aktivnosti i događaji; xiv kontinuirano praćenje sigurnosti; xv postupci otkrivanja; xvi planiranje odgovora; xvii komunikacija o odgovoru; xviii analiza odgovora; xix ublažavanje odgovora; xx poboljšanje odgovora; xxi planiranje oporavka; xxii poboljšanje oporavka; xxiii komunikacija o oporavku	i utvrđivanje; ii zaštita; iii otkrivanje; iv odgovor; v oporavak	i pravni stup; ii tehnički stup; iii organizacijski stup; iv izgradnja kapaciteta; v suradnja	i pravni i regulatorni okvir; ii gospodarski i socijalni kontekst; iii tehnološka infrastruktura; iv primjena u industriji

PRILOG B – BIBLIOGRAFIJA ANALIZE DOKUMENTACIJE

Almuhammadi, S. i Alsaleh, M. (2017.) „Information Security Model for Nist Cyber Security Framework" (Model zrelosti informacijske sigurnosti za okvir za kibersigurnost NIST-a) u Computer Science & Information Technology (CS & IT). Šesta međunarodna konferencija o konvergenciji i uslugama informacijske tehnologije, Centar za suradnju u području akademskih i industrijskih istraživanja (AIRCC).

Almuhammadi, S. i Alsaleh, M. (2017.) „Information Security Model for Nist Cyber Security Framework" (Model zrelosti informacijske sigurnosti za okvir za kibersigurnost NIST-a) u Computer Science & Information Technology (CS & IT). Dostupno na: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. i dr. (2016.) Stocktaking, analysis and recommendations on the protection of CIIs (Pregled stanja, analiza i preporuke o zaštiti ključne informatičke infrastrukture). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. i dr. (2009.) Developing Maturity Models for IT Management – A Procedure Model and its Application (Razvoj modela zrelosti za upravljanje informacijskom tehnologijom – model postupka i njegova primjena). Dostupno na: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Vlada Belgije (2012.) Strategija za kibersigurnost. Dostupno na: 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. i dr. (2018.) Developing Cybersecurity Capacity: A proof-of-concept implementation guide (Razvoj kapaciteta za kibersigurnost: vodič za provedbu dokaza koncepta) RAND Corporation. Dostupno na: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012.) „Introduction to Return on Security Investment" (Uvod u vraćanje ulaganja u sigurnost).

Sveučilište Carnegie Mellon u Pittsburghu, Sjedinjene Američke Države, Institut za softversko inženjerstvo (2019.) Model zrelosti kapaciteta u području kibersigurnosti (C2M2), verzija 2.0. Dostupno na: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Centar za sigurnosne studije (CSS), ETH Zürich (2019.), National Cybersecurity Strategies in Comparison – Challenges for Switzerland (Usporedba nacionalnih strategija za kibersigurnost – izazovi za Švicarsku). Dostupno na: 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

Vijeće ministara (2019.) Portugalski službeni list, serija 1. – br. 108 – Rezolucija Vijeća ministara br. 92/2019. Dostupno na: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016.), Cybersecurity Capacity Maturity Model for Nations (CMM) (Model zrelosti kapaciteta za kibersigurnost za države (CMM)). Sveučilište u Oxfordu.

CSIRT Maturity – Self-assessment Tool (Zrelost timova za odgovor na računalne sigurnosne incidente – alat za samoprocjenu) (nema datuma). Dostupno na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Projekt CyberCrime@IPA Vijeća Europe i Europske unije, Globalni projekt Vijeća Europe o kiberkriminalitetu i Radna skupina Europske unije za kiberkriminalitet (2011.) Specialised cybercrime units – Good practice study (Specijalizirane jedinice za kiberkriminalitet – studija dobre prakse). Dostupno na: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (Sustav za izvješćivanje i analizu kibersigurnosnih incidenata – alat za vizualnu analizu) (nema datuma). Dostupno na: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017.) Public Private Partnerships (PPP) (Javno-privatna partnerstva (JPP)).

Darra, E. (nema datuma) „Welcome to the NCSS Training Tool" (Dobro došli u alat za osposobljavanje za nacionalne strategije za kibersigurnost).

Dekker, M. A. C. (2014.) Technical Guideline on Incident Reporting (Tehničke smjernice o izvješćivanju o incidentima). Dostupno na: 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 (Tehničke smjernice o sigurnosnim mjerama). Dostupno na: 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 (Smjernice o prijetnjama i imovini). Dostupno na: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digitalna Slovenija (2016.), Strategija za kibersigurnost. Dostupno na: 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. *i dr.* (2014.) *Privacy and data protection by design - from policy to engineering* (Privatnost i integrirana zaštita podataka – od politike do inženjerstva). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Europska komisija (2012.) Uredba Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu. Dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Agencija Europske unije za mrežnu i informacijsku sigurnost (2012.) Nacionalna strategija za kibersigurnost: NCSS: Practical Guide on Development and Execution (Nacionalna strategija za kibersigurnost: Praktični vodič kroz razvoj i izvršenje). Heraklion: ENISA.

Agencija Europske unije za mrežnu i informacijsku sigurnost (2012.) NCSS: Setting the course for national efforts to strengthen security in cyberspace (Utvrđivanje smjera nacionalnih napora za jačanje sigurnosti u kiberprostoru). Heraklion: ENISA.

Agencija Europske unije za mrežnu i informacijsku sigurnost (2016.), Guidelines for SMEs on the security of personal data processing (Smjernice za MSP-ove o sigurnosti obrade osobnih podataka).

Agencija Europske unije za mrežnu i informacijsku sigurnost (2016.) NCSS good practice guide: designing and implementing national cyber security strategies (Vodič kroz dobre prakse nacionalnih strategija za kibersigurnost: osmišljavanje i provedba nacionalnih strategija za kibersigurnost). Heraklion: ENISA.

Europska unija i Agencija za mrežnu i informacijsku sigurnost (2017.) Handbook on security of personal data processing (Priručnik o sigurnosti obrade osobnih podataka). Dostupno na: http://dx.publications.europa.eu/10.2824/569768

Europska unija i Agencija za mrežnu i informacijsku sigurnost (2014.) *ENISA CERT inventory inventory of CERT teams and activities in Europe* (Popis timova za odgovor na računalne sigurnosne incidente i njihovih aktivnosti u Europi). Dostupno na: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Izvršni ured predsjednika (2015.) Memorandum za voditelje izvršnih odjela i agencija. Dostupno na: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Ured saveznog kancelara Republike Austrije (2013.) Strategija za kibersigurnost Austrije. Dostupno na: 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

Savezno ministarstvo unutarnjih poslova (2011.) Strategija kibersigurnosti za Njemačku. Dostupno na: 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 (Direktiva NIS i nacionalne (2015.) norme informacijske sigurnosti i privatnosti za MSP-ove: preporuke za poboljšanje donošenja standarda informacijske sigurnosti i privatnosti u malim i srednjim poduzećima). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Europska unija i Agencija Europske unije za mrežnu i informacijsku sigurnost (2015.) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations (Izvješće o nacionalnim i međunarodnim vježbama u području kibersigurnosti za 2015.). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Ured francuskog premijera (2014.) Francuska nacionalna strategija digitalne sigurnosti. Dostupno na: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. i dr. (2015.) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises (Norme informacijske sigurnosti i privatnosti za MSP-ove: preporuke za poboljšanje donošenja standarda informacijske sigurnosti i privatnosti u malim i srednjim poduzećima). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Sveučilište u Ghentu i dr. (2017.) „Evaluating Business Process Maturity Models" (procjena modela zrelosti poslovnih procesa), Časopis udruženja za informacijske sustave. Dostupno na: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Vlada Bugarske (2015.) Nacionalna strategija za kibersigurnost – Kiberotporna Bugarska 2020.

Vlada Hrvatske (2015.) Nacionalna strategija kibernetičke sigurnosti Republike Hrvatske. Dostupno na: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Vlada Grčke (2017.) Nacionalna strategija za kibersigurnost. Dostupno na: 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

Vlada Mađarske (2018.) Strategija za sigurnost mrežnih i informacijskih sustava. Dostupno na: 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

Vlada Irske (2019.) Nacionalna strategija za kibersigurnost. Dostupno na: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Vlada Španjolske (2019.) Nacionalna strategija za kibersigurnost. Dostupno na: 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

Institut unutarnjih revizora (ur.) (2009.) Internal audit capability model (IA-CM) for the public sector: overview and application guide (Model sposobnosti unutarnje revizije (IA-CM) za javni sektor: pregled i vodič za primjenu). Altamonte Springs, Fla: Institut unutarnjih revizora, Istraživačka zaklada.

Međunarodna unija za telekomunikacije (ITU) (2018.) Globalni indeks kibersigurnosti Dostupno na: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Međunarodna unija za telekomunikacije (ITU) (2018.) Vodič za razvoj nacionalne strategije za kibersigurnost. Dostupno na: 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" (Katarski model zrelosti kapaciteta u području kibersigurnosti), International Review of Law.

Vlada Latvije (2014.) Strategija za kibersigurnost Latvije. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Alen, A. i dr. (2014.) An evaluation framework for national cyber security strategies (Okvir za procjenu nacionalnih strategija za kibersigurnost). Heraklion: ENISA. Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. i dr. (2014,) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks* (Metodologije za utvrđivanje ključne informatičke infrastrukture i ključnih usluga: smjernice za izradu elektroničkih podatkovnih komunikacijskih mreža). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministarstvo konkurentnosti i digitalnog, pomorskog i uslužnog gospodarstva (2016.) – Strategija za kibersigurnost Malte. Dostupno na: 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

Ministarstvo gospodarstva i komunikacija (2019. Strategija za kibersigurnost– Republika Estonija). Dostupno na: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministarstvo nacionalne obrane Republike Litve (2018.) Nacionalna strategija za kibersigurnost

Nacionalni centar za kibersigurnost (2015.) Nacionalna strategija za kibersigurnost Češke. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Nacionalne strategije za kibersigurnost – interaktivna karta (nema datuma). Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Alat za procjenu nacionalnih strategija za kibersigurnost (2018.). Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Nacionalni institut za norme i tehnologiju (2018.), Framework for Improving Critical Infrastructure Cybersecurity (Okvir za poboljšanje kibersigurnosti ključne infrastrukture), verzija 1.1. Gaithersburg, MD: Nacionalni institut za norme i tehnologiju Dostupno na: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Projektna upravljačka skupina (2008.) Business Process Maturity Model (Model zrelosti poslovnog procesa). Dostupno na: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Europska unija i Zajednički istraživački centar – Europska komisija (2008.) Handbook on Constructing Composite Indicators: Methodology and User Guide (Priručnik za izradu kompozitnih pokazatelja: metodologija i priručnik za korisnike). OECD Dostupno na: https://www.oecd.org/sdd/42495745.pdf.

Ured povjerenika za elektroničke komunikacije i poštanske propise (2012.) Strategija za kibersigurnost Cipra

Službeni list Europske unije (2008.) Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=HR

Organizacija za gospodarsku suradnju i razvoj (OECD) (2012.) Cybersecurity policy making at a turning point (Donošenje politika u području kibersigurnosti na prekretnici). Dostupno na: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012.) „National Cyber Security Strategies – Practical Guide on Development and Execution" (Nacionalne strategije za kibersigurnost – praktični vodič kroz razvoj i izvršenje).

Ouzounis, E. (2012.) Good Practice Guide on National Exercises (Vodič kroz dobre prakse vježbi na nacionalnoj razini).

Portesi, S. (2017.) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects: (Poboljšanje suradnje timova za odgovor na računalne sigurnosne incidente i tijela za izvršavanje zakonodavstva: pravni i organizacijski aspekti).

Predsjedništvo Vijeća ministara (2017.) Talijanski akcijski plan za kibersigurnost. Dostupno na: 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. Dostupno na: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Vlada Rumunjske (2013.) Strategija za kibersigurnost Rumunjske. Dostupno na: 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. i Agencija Europske unije za kibersigurnost (2019.) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies (Dobre prakse u inovacijama u području kibersigurnosti u okviru nacionalne strategije za kibersigurnost). Dostupno na: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Tajništvo Odbora za sigurnost (2019.) Strategija za kibersigurnosti Finske 2019. Dostupno na: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Vlada Slovačke (2015.) Koncept kibersigurnosti Slovačke Republike. Dostupno na: 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.) Direktiva 2010/41/EU Europskog parlamenta i Vijeća od 7. srpnja 2010.

Smith, R. (2016.) Direktiva 2010/41/EU Europskog parlamenta i Vijeća od 7. srpnja 2010. u Smith, R., Temeljno zakonodavstvo EU-a. London: Macmillan Education. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L1148&from=HR.

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

Vlada Švedske (2017.) Nationell strategi för samhällets informations- och cybersäkerhet. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Vlada Danske – Ministarstvo financija (2018.) Danska strategija za kibersigurnost i informacijsku sigurnost. Dostupno na: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Savezno vijeće (2018.) Nacionalna strategija za zaštitu Švicarske od kiberrizika.

Luksemburško vladino vijeće (2018.) Nacionalna strategija za kibersigurnost. Dostupno na: 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

Vlada Nizozemske (2018.) Nacionalni program kibersigurnosti. Dostupno na: 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

Bijela kuća (2018.) Nacionalna strategija za kibersigurnost Sjedinjenih Američkih Država. Dostupno na: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P. i dr. (2011.) Izvješće Cyber Europe. Dostupno na: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. i Agencija Europske unije za mrežnu i informacijsku sigurnost (2013.) *National-level risk assessments: an analysis report* (Procjene rizika na nacionalnoj razini: izvješće o analizi). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R. i dr. (2015.) Report on cyber-crisis cooperation and management (Izvješće o suradnji i upravljanju u području kiberkrize). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A. i dr. (2015.) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises (Izvješće o suradnji i upravljanju u području kiberkrize: uobičajene prakse upravljanja krizama na razini EU-a i primjenjivost na kiberkrize). Dostupno na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Nacionalna strategija za kibersigurnost Ujedinjene Kraljevine za razdoblje 2016. – 2021. (2016.). Dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Sveučilište u Innsbrucku i dr. (2009.) Understanding Maturity Models (Razumijevanje modela zrelosti).

Wamala, D. F. (2011.), ITU National Cybersecurity Strategy Guide (Vodič ITU-a kroz nacionalne strategije za kibersigurnost). Dostupno na: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007.) „The Community Cyber Security Maturity Model" (Model zrelosti kibersigurnosti zajednice) u 2007 40th Annual Hawaii International Conference on System Sciences (40. Međunarodna konferencija o informatičkoj znanosti 2007.) (HICSS'07)

PRILOG C – OSTALI ANALIZIRANI CILJEVI

Ciljevi navedeni u nastavku analizirani su u okviru faze analize dokumentacije i razgovora koje je provela ENISA. Sljedeći ciljevi nisu dio okvira za procjenu nacionalnih kapaciteta, ali se njima razjašnjavaju teme o kojima treba raspravljati. U svakom od sljedećih potpoglavlja objasnit će se zašto je cilj odbačen.

- Razvoj sektorskih strategija za kibersigurnost
- Borba protiv kampanja dezinformiranja
- Sigurne najsuvremenije tehnologije (5G, umjetna inteligencija, kvantno računalstvo...)
- Osiguravanje suvereniteta nad podatcima
- Pružanje poticaja za razvoj industrije kiberosiguranja

Razvoj sektorskih strategija za kibersigurnost

Donošenjem sektorskih strategija usmjerenih na sektorske intervencije i poticaje svakako se uvodi jača decentralizirana sposobnost. To je osobito prikladno za države članice čiji se operatori ključnih usluga moraju baviti različitim okvirima i propisima te u kojima postoje mnoge ovisnosti zbog transverzalne prirode kibersigurnosti. Doista, u nekoliko država članica uobičajeno je uzeti u obzir desetke nacionalnih i regulatornih tijela koja poznaju posebnosti svakog sektora i imaju mandat za provedbu posebnih propisa za svaki sektor.

Danska je, na primjer, pokrenula šest ciljanih strategija usmjerenih na napore u području kibersigurnosti i informacijske sigurnosti u najvažnijim sektorima kako bi se razvio snažniji decentralizirani kapacitet u području kibersigurnosti i informacijske sigurnosti. Svaka „sektorska jedinica" doprinijet će, među ostalim, procjenama prijetnji na sektorskoj razini, praćenju, vježbama pripravnosti, uspostavi sigurnosnih sustava, razmjeni znanja i uputama. Sektorske strategije obuhvaćaju sljedeće sektore:

- energetika;
- zdravstvena skrb;
- prijevoz;
- telekomunikacije;
- financije i
- pomorski promet.

Druge države članice izrazile su interes za razmatranje sektorskih strategija za kibersigurnost kako bi se odrazili svi regulatorni zahtjevi. No treba napomenuti da takav cilj možda ne odgovara svim državama članicama ovisno o njihovoj veličini, nacionalnim politikama i zrelosti. Zbog velikih poteškoća pri osiguravanju da se okvirom obuhvate sve posebnosti ENISA nije uključila taj cilj u okvir.

Borba protiv kampanja dezinformiranja

Države članice u svoje nacionalne strategije za kibersigurnost uključuju zaštitu temeljnih načela kao što su ljudska prava, transparentnost i povjerenje javnosti. To je vrlo važno, posebno kad je riječ o dezinformacijama koje se šire putem tradicionalnih informativnih medija ili platformi društvenih medija. Osim toga, kibersigurnost je trenutačno jedan od najvećih izazova u pogledu izbora. Aktivnosti poput širenja lažnih informacija ili negativne propagande primijećene su u

različitim zemljama uoči važnih izbora. Ta prijetnja može ugroziti demokratski proces EU-a. Na europskoj razini Komisija je predstavila akcijski plan[32] za jačanje borbe protiv dezinformiranja u Europi: taj je plan usmjeren na četiri ključna područja (otkrivanje, suradnja, suradnja s internetskim platformama i podizanje svijesti) i služi izgradnji kapaciteta EU-a i jačanju suradnje među državama članicama.

četiri od 19 ispitanih zemalja izrazile su namjeru da u svojim nacionalnim strategijama suzbijanja dezinformacija i propagande razmotre pitanje dezinformiranja i propagande.

Na primjer, u francuskoj nacionalnoj strategiji za kibersigurnost[33] navodi se sljedeće: „odgovornost je države da građane informira o rizicima od manipulacije i propagande kojima se koriste zlonamjerni korisnici na internetu. Na primjer, nakon terorističkih napada na Francusku u siječnju 2015. Vlada je uspostavila informacijsku platformu o rizicima povezanima s islamskom radikalizacijom putem elektroničkih komunikacijskih mreža: Stop-djihadisme.gouv.fr." Taj bi se pristup mogao proširiti kako bi se odgovorilo na druge pojave propagande ili destabilizacije.

U drugom primjeru u nacionalnoj strategiji za kibersigurnost Poljske za razdoblje 2019. – 2024.[34] navodi se sljedeće: „protiv manipulativnog djelovanja kao što su kampanje dezinformiranja potrebno je sustavno djelovati kako bi se razvila svijest građana u kontekstu provjere autentičnosti informacija i odgovaranja na pokušaje njihova narušavanja."

Međutim, tijekom razgovora koje je provela ENISA nekoliko država članica izrazilo je mišljenje da to pitanje ne rješavaju u okviru svojih nacionalnih strategija za kibersigurnost kao kiberprijetnju, nego da se bave tim pitanjem na široj društvenoj razini, na primjer putem političkih inicijativa.

Sigurne najsuvremenije tehnologije (5G, umjetna inteligencija, kvantno računalstvo...)

Budući da se sadašnje okruženje kiberprijetnji nastavlja širiti, razvoj novih tehnologija najvjerojatnije će dovesti do povećanja intenziteta i broja kibernapada te diversifikacije metoda, sredstava i ciljeva koje upotrebljavaju subjekti koji prijete. U međuvremenu, ta nova tehnološka rješenja u obliku najsuvremenijih tehnologija imaju potencijal da postanu temelji europskog digitalnog tržišta. Kako bi se zaštitila sve veća digitalna ovisnost država članica i pojava novih tehnologija, trebalo bi uspostaviti poticaje i cjelovite politike za potporu sigurnom i pouzdanom razvoju i uvođenju tih tehnologija u EU-u.

Tijekom faze analize dokumentacije u vezi s nacionalnim strategijama za kibersigurnost država članica predstavljene su sljedeće najsuvremenije tehnologije koje su od interesa za države članice: 5G, umjetna inteligencija, kvantno računalstvo, kriptografija, računalstvo na rubu mreže, povezana i autonomna vozila, velika količina podataka i pametni podatci, lanci blokova, robotika i internet stvari.

Konkretnije, početkom 2020. Europska komisija objavila je komunikaciju u kojoj je pozvala države članice da poduzmu korake za provedbu niza mjera preporučenih u zaključcima o skupu mjera za 5G.[35] Skup mjera za 5G temelji se na Preporuci (EU) 2019/534 o kibersigurnosti 5G mreža koju je Komisija donijela 2019. i u kojoj se poziva na jedinstveni europski pristup sigurnosti 5G mreža.[36]

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32019H0534

Tijekom razgovora koje je vodila ENISA istaknuto je da je ta tema više od transverzalne teme koja se razmatra u nacionalnoj strategiji za kibersigurnost, a ne kao poseban cilj sam po sebi.

Osiguravanje suvereniteta nad podatcima

S jedne strane, kiberprostor se može smatrati golemim globalnim zajedničkim prostorom koji je lako dostupan i omogućuje visok stupanj povezanosti i velike mogućnosti za društveno-gospodarski rast. S druge strane, kiberprostor karakterizira i slaba nadležnost, poteškoće pri pripisivanju određenih radnji, nedostatak granica i međusobno povezani sustavi koji mogu biti porozni i čiji se podatci mogu ukrasti ili kojima čak mogu pristupiti strane vlade. Osim tih dvaju perspektiva, digitalni ekosustav obilježen je koncentracijom internetskih platformi i infrastrukture u rukama vrlo malog broja dionika. Svi navedeni aspekti navode države članice na promicanje digitalnog suvereniteta. Postizanje digitalnog suvereniteta znači da građani i poduzeća mogu u potpunosti napredovati upotrebom digitalnih usluga i proizvoda IKT-a koji su pouzdani, bez straha za osobne podatke ili digitalnu imovinu, ekonomsku autonomiju ili politički utjecaj.

Suverenost podataka ili digitalni suverenitet zagovaraju države članice na nacionalnoj i na europskoj razini. Iako se čini da države članice to pitanje ne rješavaju izravno u okviru svojih nacionalnih strategija za kibersigurnost kao poseban cilj, rješavaju ga kao transverzalno načelo ili navode svoju namjeru da osiguraju digitalni suverenitet na nacionalnoj razini u *ad hoc* publikacijama usmjeravanjem na ključne tehnologije. Na primjer, u francuskom strateškom pregledu kiberobrane za 2018. navodi se da je „nadzor sljedećih tehnologija od ključne važnosti za osiguravanje digitalnog suvereniteta: šifriranje komunikacije, otkrivanje kibernapada, profesionalni mobilni radio, računalstvo u oblaku i umjetna inteligencija”.[37]

Na europskoj razini države članice aktivno sudjeluju u definiranju europske strategije za podatke (COM/2020/66 final) i izgradnji okvira EU-a za certifikaciju digitalnih proizvoda, usluga i procesa IKT-a uspostavljenog Aktom EU-a o kibersigurnosti (2019/881) kako bi se osigurala strateška digitalna autonomija na europskoj razini.

Faza razgovora s državama članicama pokazala je da se tema digitalnog suvereniteta često smatra širim pitanjem od onog koje je ograničeno na kibersigurnost. Stoga države članice tu temu ne obuhvaćaju svojim nacionalnim strategijama za kibersigurnost, a neke od njih tu temu ne obuhvaćaju kao poseban cilj sam po sebi.

Pružanje poticaja razvoju industrije kiberosiguranja

Sadašnje stanje industrije kiberosiguranja pokazuje da je svjetsko tržište nedvojbeno naraslo. No ono je još u začetku s obzirom na to da se podatci moraju i dalje prikupljati te da je i dalje potrebno postaviti brojne presedane (npr. „tiho pokriće”, sistemski kiberrizici...). Nadalje, procijenjeni gubitci od kibernapada diljem svijeta veći su za nekoliko redova veličine od postojećeg kapaciteta pokrivenosti sektora kiberosiguranja (Radni dokument MMF-a – kiberrizik za financijski sektor: Okvir za kvantitativnu procjenu, WP/18/143). Međutim, razvoj industrije kiberosiguranja zasigurno može donijeti koristi i postaviti temelje za uspješne mehanizme. Doista, mehanizmi kiberosiguranja mogu pomoći pri sljedećem:

- podizanju svijesti o kibersigurnosnim rizicima u poduzećima;
- kvantitativnoj procjeni izloženosti kiberrizicima;
- poboljšanju upravljanja rizicima u području kibersigurnosti;
- pružanju potpore organizacijama koje su žrtve kibernapada i
- naknadi štete (materijalne ili nematerijalne) uzrokovane kibernapadom.

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

Određene države članice počele su raditi na tom pitanju. Na primjer:

- Estonija je u svojoj nacionalnoj strategiji za kibersigurnost zauzela tzv. stav „čekaj i vidi”: „Kako bi se ublažili kiberrizici u privatnom sektoru općenito, analizirat će se potražnja i ponuda usluga kiberosiguranja u Estoniji te će se na temelju toga dogovoriti kooperativna načela za povezane stranke, uključujući razmjenu informacija, pripremu procjene rizika itd. Danas su pružatelji usluga kiberosiguranja malobrojni na estonskom tržištu i potrebno je najprije utvrditi tko što nudi. Složenost zaštite osiguranjem često se smatra preprekom razvoju tržišta kiberosiguranja.”
- Luksemburg u svojoj nacionalnoj strategiji za kibersigurnost posebno podržava razvoj industrije kiberosiguranja: „1. cilj: stvaranje novih proizvoda i usluga. Kako bi se ujedinili rizici i potaknulo žrtve digitalnih kiberincidenata da potraže pomoć stručnjaka u upravljanju incidentom i ponovnoj uspostavi sustava pogođenog zlonamjernim činom, osiguravajuća društva poticat će se na stvaranje posebnih proizvoda za područje kiberosiguranja.”

Povratne informacije ispitanika bile su prilično raznolike kad je riječ o toj temi: neke države članice izjavile su da je pitanje kiberosiguranja nedavno postalo tema rasprave, dok su se druge složile da, iako je ta tema obećavajuća, industrija još nije dovoljno razvijena. Međutim, velik broj ispitanika izjavio je da se ta tema ne rješava u okviru nacionalne strategije za kibersigurnost, bilo zato što se smatralo da je previše specifična ili nije obuhvaćena područjem primjene nacionalne strategije za kibersigurnost.

TP-06-20-047-HR-N

O Agenciji Europske unije za kibersigurnost

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije posvećena postizanju visoke zajedničke razine kibersigurnosti diljem Europe. Agencija Europske unije za kibersigurnost osnovana je 2004. na temelju Akta o kibersigurnosti EU-a i odonda pridonosi kiberpolitici EU-a, poboljšava pouzdanost proizvoda, usluga i postupaka IKT-a s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi na kiberizazove koji je očekuju u budućnosti. Razmjenom znanja, izgradnjom kapaciteta i informiranjem Agencija zajedno sa svojim ključnim dionicima radi na jačanju povjerenja u povezano gospodarstvo kako bi se povećala otpornost infrastrukture Unije te u konačnici zaštitila sigurnost europskog društva i građana. Više informacija dostupno je na: 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 978-92-9204-480-0
DOI: 10.2824/19