EUROPEAN UNION AGENCY
FOR CYBERSECURITY

OKVIR ZA OCENJEVANJE NACIONALNIH ZMOGLJIVOSTI

DECEMBER 2020

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost, ENISA, je agencija Unije, katere cilj je dosegati visoko skupno raven kibernetske varnosti po vsej Evropi. Ustanovljena je bila leta 2004, njene pristojnosti pa so bile okrepljene z uredbo EU o kibernetski varnosti. Prispeva h kibernetski politiki EU, povečuje zaupanje v produkte, storitve in procese IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi, da bo pripravljena na kibernetske izzive prihodnosti. Z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter na koncu zagotovila digitalno varnost evropske družbe in državljanov. Za več informacij obiščite spletno stran www.enisa.europa.eu.

KONTAKT

Če želite stopiti v stik z avtorji, pišite na team@enisa.europa.eu.
Če imate novinarsko vprašanje v zvezi s tem dokumentom, pišite na press@enisa.europa.eu.

AVTORJI

Anna Sarri, Pinelopi Kyranoudi – Agencija Evropske unije za kibernetsko varnost (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

ZAHVALA

Agencija ENISA se zahvaljuje vsem sodelujočim strokovnjakom, ki so dodali dragocen prispevek k temu poročilu, zlasti naslednjim (naštetim po abecednem vrstnem redu):

Center za kibernetsko varnost (Belgija)

CFCS – Center for Cybersikkerhed (Danska), Thomas Wulff

Evropski center za boj proti kibernetski kriminaliteti – EC3, Adrian-Ionut Bobeica

Evropski center za boj proti kibernetski kriminaliteti – EC3, Alzofra Martinez Alvaro

Italijanska vlada (Italija)

Malteška agencija za informacijsko tehnologijo (Malta Information Technology Agency) (Malta), Katia Bonello in Martin Camilleri

Ministrstvo za digitalno upravljanje (Grčija), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali in Sotiris Vasilos

Ministrstvo za gospodarske zadeve in komunikacijo (Estonija), Anna-Liisa Pärnalaas

Ministrstvo za pravosodje in javno varnost (Norveška), Robin Bakke

Nacionalna agencija za kibernetsko in informacijsko varnost (Češka republika), Veronika Netolická

Nacionalni varnostni organ (Slovaška)

NCTV, Ministrstvo za pravosodje in varnost (Nizozemska)

Oddelek za nacionalno varnost (Španija), Maria Mar Lopez Gil

Oddelek za politiko kibernetske varnosti, Služba za okolje, podnebje in komunikacijo (Cyber Security Policy Division, Department of Environment, Climate and Communications) (Irska), James Caffrey

Osrednji državni urad za razvoj digitalne družbe (Hrvaška), Marin Ante Pivčević

Portugalski nacionalni center za kibernetsko varnost (Portugalska), Alexandre Leite in Pedro Matos

Univerza v Oxfordu – Svetovni center za zmogljivosti na področju kibernetske varnosti (Global Cyber Security Capacity Centre), Carolin Weisser Harris

Uprava za informacijsko varnost (Republika Slovenija), Marjan Kavčič

Zvezno ministrstvo za notranje zadeve (Nemčija), Sascha-Alexander Lettgen

Agencija ENISA se za dragocen prispevek k tej študiji zahvaljuje tudi vsem sodelujočim strokovnjakom, ki so želeli ostati anonimni.

PRAVNO OBVESTILO

OBVESTILO O AVTORSKIH PRAVICAH

ISBN: 978-92-9204-494-7

DOI: 10.2824/380323

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

1. KAZALO

GLOSAR IZRAZOV

KRATICA	OPREDELITEV
C2M2	Zrelostni model za zmogljivosti na področju kibernetske varnosti (Cybersecurity Capability Maturity Model)
CCRA	Dogovor o priznavanju skupnih meril (Common Criteria Recognition Arrangement)
CCSMM	Zrelostni model kibernetske varnosti skupnosti (The Community Cybersecurity Maturity Model)
CII	Kritična informacijska infrastruktura (Critical Information Infrastructure)
CMM	Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (Cybersecurity Capacity Maturity Model for Nations)
CMMC	Certificiranje zrelosti na področju kibernetske varnosti (Cybersecurity Maturity Model Certification)
CPI	Indeks kibernetske moči (Cyber Power Index)
CSIRT	Skupine za odzivanje na incidente na področju računalniške varnosti (Computer Security Incident Response Teams)
CVD	Usklajeno razkrivanje šibkih točk (Coordinated Vulnerability Disclosure)
DČ	Država članica
ECCG	Evropska certifikacijska skupina za kibernetsko varnost (European Cybersecurity Certification Group)
ECSM	Evropski mesec kibernetske varnosti (European Cybersecurity Month)
ECSO	Evropska organizacija za kibernetsko varnost (European Cyber Security Organisation)
EDT	Enotni digitalni trg
EFTA	Evropsko združenje za prosto trgovino
EOK	Evropsko ogrodje kvalifikacij
EU	Evropska unija
GCI	Svetovni indeks kibernetske varnosti (Global Cybersecurity Index)
GDPR	Splošna uredba o varstvu podatkov
GDS	Vladna digitalna služba (Government Digital Service)
IA-CM	Model službe za notranjo revizijo za javni sektor (Internal Audit Capability Model for the Public Sector)
IKT	Informacijske in komunikacijske tehnologije
ISMM	Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (Information Security Maturity Model for NIST Cybersecurity Framework)

ITU	Mednarodna telekomunikacijska zveza (International Telecommunication Union)
JZP	Javno-zasebna partnerstva (Public-private partnerships)
LEA	Organ kazenskega pregona (Law Enforcement Agency)
MSP	Mala in srednja podjetja
NCSS	Nacionalne strategije za kibernetsko varnost (National Cybersecurity Strategies)
NIS	Varnost omrežij in informacij (Network and Information Security)
NIST	Nacionalni inštitut za standarde in tehnologijo
NLO	Nacionalni uradniki za zvezo (National Liaison Officers)
OES	Izvajalci bistvenih storitev (Operators of Essential Services)
OT	Operativna tehnologija
PET	Tehnologije za boljše varovanje zasebnosti (Privacy Enhancing Technologies)
PIMS	Sistem za upravljanje osebnih podatkov (Privacy Information Management System)
Q-C2M2	Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Qatar Cybersecurity Capability Maturity Model)
R in R	Raziskave in razvoj
SOG-IS MRA	Skupina visokih uradnikov za varnost informacijskih sistemov, Sporazum o vzajemnem priznavanju (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement)
UI	Umetna inteligenca
ZOVP	Zakon o varstvu podatkov (Data Protection Act)

POVZETEK

Ker se sedanje okolje kibernetskih groženj še naprej širi in kibernetski napadi še naprej naraščajo po intenzivnosti in številu, se morajo države članice EU učinkovito odzvati z nadaljnjim razvojem in prilagajanjem svojih nacionalnih strategij za kibernetsko varnost (NCSS). Odkar je agencija ENISA leta 2012 objavila prve študije, povezane z nacionalnimi strategijami za kibernetsko varnost, so države članice EU in države EFTA dosegle velik napredek pri razvoju in izvajanju svojih strategij.

V tem poročilu je predstavljeno delo, ki ga je opravila agencija ENISA pri oblikovanju okvirja za ocenjevanje nacionalnih zmogljivosti (NCAF).

Namen okvirja je državam članicam pomagati pri samoocenjevanju njihove ravni zrelosti z ocenjevanjem ciljev njihovih nacionalnih strategij za kibernetsko varnost, kar jim bo v pomoč pri krepitvi in razvoju zmogljivosti na področju kibernetske varnosti tako na strateški kot operativni ravni.

Okvir predstavlja preprost reprezentativen pregled ravni zrelosti posamezne države članice na področju kibernetske varnosti. Okvir za ocenjevanje nacionalnih zmogljivosti (NCAF) je orodje, ki državam članicam pomaga:

- pridobiti koristne informacije za razvoj dolgoročne strategije (npr. dobre prakse, smernice);
- prepoznati manjkajoče elemente v nacionalni strategiji za kibernetsko varnost;
- dodatno okrepiti zmogljivosti na področju kibernetske varnosti;
- sprejemati odgovornost pri političnih ukrepih;
- zagotoviti verodostojnost pred širšo javnostjo in mednarodnimi partnerji;
- pri ozaveščanju in izboljšanju javne podobe organizacije kot pregledne organizacije;
- predvidevati prihodnje problematike;
- opredeliti pridobljene izkušnje in dobre prakse;
- zagotoviti skupno izhodišče na področju zmogljivosti kibernetske varnosti po vsej EU z namenom olajšanja razprav in
- oceniti nacionalne zmogljivosti na področju kibernetske varnosti.

Ta okvir je bil oblikovan ob podpori strokovnjakov agencije ENISA ter predstavnikov iz 19 držav članic in držav EFTA[1]. Ciljna skupina tega poročila so oblikovalci politik, strokovnjaki in vladni uradniki, ki so odgovorni za ali vključeni v oblikovanje, izvajanje in ocenjevanje nacionalne

[1] Opravljeni so bili razgovori s predstavniki naslednjih držav članic in držav EFTA: Belgija, Hrvaška, Češka republika, Danska, Estonija, Nemčija, Grčija, Madžarska, Irska, Italija, Lihtenštajn, Malta, Nizozemska, Norveška, Portugalska, Slovaška, Slovenija, Španija, Švedska.

strategije za kibernetsko varnost ter, na širši ravni, zmogljivosti na področju kibernetske varnosti.

Okvir za ocenjevanje nacionalnih zmogljivosti zajema 17 strateških ciljev in je sestavljen iz štirih glavnih sklopov:

- Sklop 1: Upravljanje in standardi kibernetske varnosti
  1. Razvoj nacionalnega načrta za odzivanje na kibernetske grožnje
  2. Določitev osnovnih varnostnih ukrepov
  3. Varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve

- Sklop 2: Krepitev zmogljivosti in ozaveščanje
  4. Organiziranje vaj na področju kibernetske varnosti
  5. Vzpostavitev zmogljivosti za odzivanje na incidente
  6. Ozaveščanje uporabnikov
  7. Okrepitev programov usposabljanja in izobraževanja
  8. Spodbujanje raziskav in razvoja
  9. Zagotavljanje spodbud zasebnemu sektorju za naložbe v varnostne ukrepe
  10. Izboljšanje kibernetske varnosti dobavne verige

- Sklop 3: Pravo in regulativa
  11. Varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in DSP
  12. Obravnavanje kibernetske kriminalitete
  13. Vzpostavitev mehanizmov za poročanje o incidentih
  14. Okrepitev zasebnosti in varstva podatkov

- Sklop 4: Sodelovanje
  15. Vzpostavitev javno-zasebnega partnerstva
  16. Institucionalizacija sodelovanja med javnimi agencijami
  17. Mednarodno sodelovanje

1. UVOD

Direktiva o varnosti omrežij in informacij, objavljena julija 2016, od držav članic EU zahteva, da sprejmejo nacionalno strategijo za varnost omrežij in informacijskih sistemov, imenovano tudi nacionalna strategija za kibernetsko varnost, kot je določeno v členih 1 in 7. V povezavi s tem je nacionalna strategija za kibernetsko varnost opredeljena kot okvir, ki določa strateška načela, smernice, strateške cilje, prednostne naloge, ustrezne politike in regulativne ukrepe. Predvideni cilj nacionalne strategije za kibernetsko varnost je doseči in ohraniti visoko raven varnosti omrežij in sistemov ter tako državam članicam omogočiti, da ublažijo morebitne nevarnosti. Poleg tega je lahko nacionalna strategija za kibernetsko varnost tudi katalizator za industrijski razvoj ter gospodarski in družbeni napredek.

V Aktu EU o kibernetski varnosti je navedeno, da agencija ENISA spodbuja razširjanje najboljših praks pri opredeljevanju in izvajanju nacionalne strategije za kibernetsko varnost s podpiranjem držav članic pri sprejemanju Direktive o varnosti omrežij in informacij ter z zbiranjem dragocenih povratnih informacij o njihovih izkušnjah. V ta namen je agencija ENISA razvila več orodij za pomoč državam članicam pri razvoju, izvajanju in ocenjevanju njihovih nacionalnih strategij za kibernetsko varnost.

Agencija ENISA si v okviru svojega mandata prizadeva razviti okvir za samoocenjevanje nacionalnih zmogljivosti, ki bo namenjen merjenju ravni zrelosti različnih nacionalnih strategij za kibernetsko varnost. Cilj tega poročila je predstaviti izvedeno študijo, katere cilj je bil opredeliti okvir za samoocenjevanje.

1.1 PODROČJE UPORABE IN CILJI ŠTUDIJE

Glavni cilj te študije je vzpostaviti okvir za samoocenjevanje nacionalnih zmogljivosti, v nadaljnjem besedilu okvir NCAF, za merjenje ravni zrelosti držav članic na področju zmogljivosti kibernetske varnosti. Natančneje, okvir bi moral državam članicam omogočiti, da:

- izvajajo ocenjevanja svojih nacionalnih zmogljivosti na področju kibernetske varnosti;
- povečajo ozaveščenost o ravni zrelosti države;
- opredelijo področja, na katerih so potrebne izboljšave, in
- okrepijo zmogljivosti na področju kibernetske varnosti.

Ta okvir bi moral državam članicam in zlasti nacionalnim oblikovalcem politik pomagati pri izvedbi vaje iz samoocenjevanja, katere namen je izboljšati nacionalne zmogljivosti na področju kibernetske varnosti.

1.2 METODOLOŠKI PRISTOP

Metodološki pristop, ki je bil uporabljen za razvoj okvirja za samoocenjevanje nacionalnih zmogljivosti, temelji na štirih glavnih korakih:

1. **Teoretične raziskave**: prvi korak je vključeval pregled obsežne literature, da bi zbrali najboljše prakse v zvezi z razvojem okvirja za ocenjevanje zrelosti nacionalnih strategij kibernetske varnosti. Teoretična raziskava se osredotoča na sistematično analizo ustreznih dokumentov o krepitvi zmogljivosti in opredelitvi strategije na področju kibernetske varnosti, na obstoječe nacionalne strategije za kibernetsko varnost držav članic in na primerjavo obstoječih zrelostnih modelov na področju kibernetske varnosti. Primerjalna analiza obstoječih zrelostnih modelov je bila izvedena s sprejetjem okvirja

analize, razvitega za namene te študije. Okvir analize temelji na Beckerjevi[2] metodologiji za razvoj zrelostnih modelov, ki določa splošni in konsolidirani model postopka za oblikovanje zrelostnih modelov ter jasne zahteve za razvoj le-teh. Okvir analize je bil dodatno prilagojen, da izpolnjuje potrebe te študije.

2. **Izbor strokovnjakov in stališča deležnikov:** na podlagi podatkov, zbranih s pomočjo teoretične raziskave, in povezanih predhodnih ugotovitev analize je ta faza vključevala opredelitev strokovnjakov, ki imajo izkušnje z razvojem in izvajanjem nacionalnih strategij za kibernetsko varnost ali zrelostnih modelov, in povabilo le-teh k razgovoru. Agencija ENISA se je obrnila na svojo skupino strokovnjakov za nacionalne strategije kibernetske varnosti in na nacionalne uradnike za zvezo, da bi poiskala ustrezne strokovnjake v posamezni državi članici. Poleg tega so bili opravljeni razgovori z nekaterimi strokovnjaki, ki so sodelovali pri razvoju zrelostnih modelov. Skupaj je bilo opravljenih 22 razgovorov, od katerih jih je bilo 19 opravljenih s predstavniki agencij za kibernetsko varnost iz različnih držav članic (in držav EFTA).
3. **Analiza zbranih podatkov o oceni stanja:** podatki, zbrani s pomočjo teoretične raziskave in razgovorov, so bili nato analizirani, da bi se opredelile najboljše prakse pri zasnovi okvirja za samoocenjevanje, namenjenega merjenju zrelosti nacionalnih strategij za kibernetsko varnost, da bi razumeli potrebe držav članic in določili, katere podatke je mogoče zbrati v različnih evropskih državah[3]. Na podlagi te analize je bilo mogoče izpopolniti predhodni model, ki je bil razvit v prejšnjih fazah, in izpopolniti sklop kazalnikov, vključenih v model, ravni zrelosti in njihove razsežnosti.
4. **Dokončno oblikovanje modela:** strokovnjaki agencije ENISA s predmetnega področja so nato pregledali posodobljeno različico okvirja za samoocenjevanje nacionalnih zmogljivosti, nato pa so jo pred objavo dodatno potrdili strokovnjaki na delavnici, ki je bila izvedena oktobra 2020.

1.3 CILJNA SKUPINA

Ciljna skupina tega poročila so oblikovalci politik, strokovnjaki in vladni uradniki, ki so odgovorni za ali vključeni v oblikovanje, izvajanje in ocenjevanje nacionalne strategije za kibernetsko varnost ter, na širši ravni, zmogljivosti na področju kibernetske varnosti. Poleg tega so lahko ugotovitve, ki so formalizirane v tem dokumentu, koristne za strokovnjake na področju politike kibernetske varnosti in raziskovalce na nacionalni ali evropski ravni.

[2] J. Becker, R. Knackstedt in J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application" *(Razvoj zrelostnih modelov za upravljanje IT: Model postopka in njegova uporaba)*, Business & Information Systems Engineering, let. 1, št. 3, str. 213–222, Junij 2009.
[3] Za namene te raziskave „evropske države", navedene v tem poročilu, vključujejo 27 držav članic EU.

2. OZADJE

2.1 PREDHODNO DELO V ZVEZI Z ŽIVLJENJSKIM CIKLOM NACIONALNE STRATEGIJE ZA KIBERNETSKO VARNOST

Kot je navedeno v Aktu EU o kibernetski varnosti, je eden od glavnih ciljev agencije ENISA podpirati države članice pri razvoju nacionalnih strategij za varnost omrežij in informacijskih sistemov, spodbujati razširjanje teh strategij in spremljati njihovo izvajanje. Agencija ENISA je v okviru svojega mandata pripravila več dokumentov o tej temi, da bi spodbudila izmenjavo dobrih praks in podprla izvajanje nacionalnih strategij za kibernetsko varnost po vsej EU:

- „Praktični vodnik za razvojno in izvedbeno fazo nacionalne strategije za kibernetsko varnost“,[4] objavljen leta 2012;
- „Določitev poti za nacionalna prizadevanja za okrepitev varnosti v kibernetskem prostoru“,[5] objavljeno leta 2012;
- prvi okvir agencije ENISA za ocenjevanje nacionalnih strategij za kibernetsko varnost držav članic, objavljen[6] leta 2014;
- „Spletni interaktivni zemljevid nacionalnih strategij za kibernetsko varnost“,[7] objavljen leta 2014;
- „Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost“,[8] objavljen leta 2016;
- „Orodje za ocenjevanje nacionalnih strategij za kibernetsko varnost“,[9] objavljeno leta 2018;
- „Dobre prakse pri inovacijah na področju kibernetske varnosti v okviru nacionalne strategije za kibernetsko varnost“,[10] objavljen leta 2019.

PRILOGA A vsebuje kratek povzetek glavnih publikacij agencije ENISA o tej temi.

Zgoraj navedeni vodniki in dokumenti so bili proučeni v okviru teoretične raziskave. Zlasti „Orodje za ocenjevanje nacionalnih strategij za kibernetsko varnost“[11] je temeljni element

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, posodobljeno 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Ta dokument posodablja vodnik iz leta 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost: oblikovanje in izvajanje nacionalnih strategij za kibernetsko varnost) (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

okvirja za ocenjevanje nacionalnih zmogljivosti (NCAF). Okvir NCAF temelji na ciljih, ki so zajeti v spletnem ocenjevalnem orodju za nacionalne strategije kibernetske varnosti.

2.2 SKUPNI CILJI, OPREDELJENI V OKVIRU EVROPSKIH NACIONALNIH STRATEGIJ ZA KIBERNETSKO VARNOST

Zaradi razlik med posameznimi državami članicami je težko opredeliti skupne dejavnosti ali akcijske načrte v različnih nacionalnih in pravnih okvirjih ter političnih agendah. Vendar pa imajo nacionalne strategije za kibernetsko varnost držav članic pogosto zastavljene strateške cilje, ki se nanašajo na iste teme. Tako je bilo na podlagi predhodnega dela agencije ENISA in analize nacionalnih strategij za kibernetsko varnost držav članic opredeljenih 22 strateških ciljev. Petnajst od teh strateških ciljev je bilo opredeljenih že v okviru predhodnega gradiva agencije ENISA, dva sta bila na novo dodana v tej študiji, pet ciljev pa je bilo opredeljenih za razmislek v prihodnosti.

2.2.1 Skupni strateški cilji, ki jih zajemajo strategije držav članic

Na podlagi predhodnega gradiva agencije ENISA, tj. orodja za ocenjevanje nacionalnih strategij za kibernetsko varnost[12], je v naslednji preglednici prikazan zgoraj navedeni sklop 15 strateških ciljev, ki so običajno zajeti v nacionalnih strategijah za kibernetsko varnost držav članic. Cilji določajo jedro splošne „nacionalne filozofije“ na to temo. Dodatne informacije o ciljih, opisanih v nadaljevanju, so na voljo v poročilu agencije ENISA: „Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost“[13].

Preglednica 1: Skupni strateški cilji, ki jih zajemajo nacionalne strategije za kibernetsko varnost posameznih držav članic

ID	Strateški cilji nacionalne strategije za kibernetsko varnost	Cilji
1	Razvoj nacionalnih načrtov za odzivanje na kibernetske grožnje	▶ predstaviti in pojasniti merila, ki bi jih bilo treba uporabiti za opredelitev situacije kot krize; ▶ opredelitev ključnih procesov in ukrepov za obvladovanje krize in ▶ jasna opredelitev vlog in odgovornosti različnih deležnikov med kibernetsko krizo; ▶ predstaviti in pojasniti merila za razglasitev konca krize in/ali za določitev, kdo je pristojen, da ga razglasi.
2	Določitev osnovnih varnostnih ukrepov	▶ uskladitev različnih praks organizacij v javnem in zasebnem sektorju; ▶ oblikovanje skupnega jezika med pristojnimi javnimi organi in organizacijami ter odprtih varnih komunikacijskih kanalov; ▶ različnim deležnikom omogočiti, da preverijo in primerjajo svoje zmogljivosti na področju kibernetske varnosti; ▶ izmenjava informacij o dobrih praksah na področju kibernetske varnosti v vseh industrijskih sektorjih in ▶ pomoč deležnikom pri prednostnem razvrščanju njihovih naložb v varnost.
3	Organiziranje vaj na področju kibernetske varnosti	▶ opredelitev, kaj je treba testirati (načrti in postopki, ljudje, infrastruktura, zmogljivosti odzivanja, zmogljivosti sodelovanja, komunikacija itd.); ▶ vzpostavitev nacionalne skupine za načrtovanje vaj na področju kibernetske varnosti, skupina naj ima jasno opredeljen mandat in

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Ta dokument posodablja vodnik iz leta 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost: oblikovanje in izvajanje nacionalnih strategij za kibernetsko varnost) (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strateški cilji nacionalne strategije za kibernetsko varnost	Cilji
		▶ vključitev vaj na področju kibernetske varnosti v življenjski cikel nacionalne strategije za kibernetsko varnost ali nacionalnega načrta za odzivanje na kibernetske grožnje.
4	Vzpostavitev zmogljivosti za odzivanje na incidente	▶ mandat – ta se nanaša na pooblastila, vloge in odgovornosti, ki jih mora zadevna vlada dodeliti skupini; ▶ portfelj storitev – zajema storitve, ki jih skupina zagotavlja svojim pooblastiteljem ali jih uporablja za svoje notranje delovanje; ▶ operativne zmogljivosti – se nanašajo na tehnične in operativne zahteve, ki jih mora izpolnjevati skupina, in ▶ sposobnost sodelovanja – vključuje zahteve glede izmenjave informacij z drugimi skupinami, ki niso zajete v prejšnjih treh kategorijah, npr. oblikovalci politik, vojska, regulatorji, operaterji (kritična informacijska infrastruktura) in organi kazenskega pregona.
5	Ozaveščanje uporabnikov	▶ opredelitev vrzeli v znanju v zvezi s kibernetsko varnostjo ali v zvezi z vprašanji informacijske varnosti in ▶ zapolnitev teh vrzeli s pomočjo ozaveščanja ali z razvojem/krepitvijo temeljev znanja.
6	Okrepitev programov usposabljanja in izobraževanja	▶ okrepitev operativne zmogljivosti obstoječe delovne sile na področju informacijske varnosti; ▶ spodbujati študente, da se vključijo v izobraževanje na področju kibernetske varnosti in jih nato pripraviti na delo na tem področju; ▶ podpirati in spodbujati odnose med akademskim okoljem na področju informacijske varnosti in industrijo informacijske varnosti ter ▶ usklajevanje usposabljanja na področju kibernetske varnosti s potrebami podjetij.
7	Spodbujanje raziskav in razvoja	▶ opredelitev dejanskih vzrokov za ranljivosti, namesto popravljanja njihovega učinka; ▶ povezovanje znanstvenikov z različnih področij, da se zagotovijo rešitve za večdimenzionalne in kompleksne težave, kot so fizične kibernetske grožnje; ▶ povezovati potrebe industrije z izsledki raziskav ter tako olajšati prehod iz teorije v prakso; ▶ poiskati načine za ohranjanje, pa tudi za povečanje ravni kibernetske varnosti izdelkov in storitev, ki podpirajo obstoječo kibernetsko infrastrukturo.
8	Zagotavljanje spodbud zasebnemu sektorju za naložbe v varnostne ukrepe	▶ opredelitev možnih spodbud zasebnim podjetjem za naložbe v varnostne ukrepe; ▶ podjetjem zagotoviti spodbude, da se bodo odločala za naložbe v varnost.
9	Varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in ponudnikov digitalnih storitev (kritična informacijska infrastruktura)	▶ opredelitev kritične informacijske infrastrukture; ▶ opredelitev in zmanjšanje zadevnih tveganj za kritično informacijsko infrastrukturo.
10	Obravnavanje kibernetske kriminalitete	▶ oblikovanje zakonov na področju kibernetske kriminalitete; ▶ povečanje učinkovitosti organov kazenskega pregona.
11	Vzpostavitev mehanizmov za poročanje o incidentih	▶ pridobivanje znanja o splošnem okolju, v katerem obstaja nevarnost; ▶ ocena učinka incidentov (npr. kršitev varnosti, izpadov omrežja, prekinitev storitev); ▶ pridobivanje znanja o obstoječih in novih ranljivostih in o vrstah napadov; ▶ ustrezna posodobitev varnostnih ukrepov; ▶ izvajanje določb iz direktive o varnosti omrežij in informacij, ki se nanašajo na poročanje o incidentih.
12	Okrepitev zasebnosti in varstva podatkov	▶ prispevati h krepitvi temeljnih pravic glede zasebnosti in varstva podatkov.

ID	Strateški cilji nacionalne strategije za kibernetsko varnost	Cilji
13	Vzpostavitev javno-zasebnega partnerstva (JZP)	▶ odvračanje (za odvračanje napadalcev); ▶ zaščita (uporablja raziskave o novih varnostnih grožnjah); ▶ odkrivanje (uporablja izmenjavo informacij za obravnavanje novih groženj); ▶ odzivanje (zagotovitev zmogljivosti za obvladovanje začetnih posledic incidenta); ▶ okrevanje (zagotovitev zmogljivosti za odpravo končnega učinka incidenta).
14	Institucionalizacija sodelovanja med javnimi agencijami	▶ povečati sodelovanje med javnimi agencijami, ki imajo odgovornost in pristojnost na področju kibernetske varnosti; ▶ preprečevanje prekrivanja med javnimi agencijami glede pristojnosti in virov; ▶ izboljšanje in institucionalizacija sodelovanja med javnimi agencijami na različnih področjih kibernetske varnosti.
15	Mednarodno sodelovanje (ne le med državami članicami EU)	▶ pridobiti koristi od oblikovanja skupne baze znanja med državami članicami EU; ▶ ustvarjanje sinergijskih učinkov med nacionalnimi organi za kibernetsko varnost in ▶ omogočanje in okrepitev boja proti mednarodnemu kriminalu.

2.2.2 Dodatni strateški cilji

Na podlagi teoretičnih raziskav in razgovorov, ki jih je opravila agencija ENISA, so bili opredeljeni dodatni strateški cilji. Države članice te teme čedalje bolj obravnavajo v svojih nacionalnih strategijah za kibernetsko varnost oziroma opredeljujejo akcijske načrte o isti zadevi. Navedeni so tudi primeri dejavnosti, ki jih izvajajo države članice. Če je primer vzet iz javno dostopnega vira, je naveden sklic. Kadar pa primeri temeljijo na zaupnih razgovorih z uradniki držav članic EU, sklici niso navedeni.

Opredeljeni so bili naslednji dodatni strateški cilji:

- izboljšanje kibernetske varnosti dobavne verige in
- varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve.

Izboljšanje kibernetske varnosti dobavne verige

Mala in srednje velika podjetja (MSP) so hrbtenica evropskega gospodarstva. Predstavljajo 99 % vseh podjetij v EU[14], leta 2015 pa je bilo ocenjeno, da so MSP ustvarila približno 85 % novih delovnih mest in zagotovila dve tretjini vseh delovnih mest v zasebnem sektorju v EU. Poleg tega MSP zagotavljajo storitve velikim podjetjem in vedno bolj sodelujejo z javnimi upravami[15], zato je treba opozoriti, da MSP v današnjem medsebojno povezanem okolju predstavljajo šibek člen za kibernetske napade. MSP so namreč najbolj izpostavljena kibernetskim napadom, vendar si pogosto ne morejo privoščiti, da bi ustrezno vlagala v

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
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

kibernetsko varnost[16]. Izboljšanje kibernetske varnosti dobavne verige bi bilo zato treba izvajati s poudarkom na MSP.

Poleg tega sistemskega pristopa lahko države članice okrepijo tudi prizadevanja za kibernetsko varnost posebnih storitev in proizvodov IKT, ki veljajo za bistvene: tehnologije IKT, ki se uporabljajo v kritični informacijski infrastrukturi, varnostni mehanizmi, ki se uveljavljajo v telekomunikacijskem sektorju (nadzor na ravni ponudnikov internetnih storitev itd.), skrbniške storitve, kot so opredeljene v uredbi eIDAS, in ponudniki storitev v oblaku. Poljska se je na primer v svoji nacionalni strategiji za kibernetsko varnost[17] za obdobje 2019–2024 zavezala, da bo razvila nacionalni sistem za ocenjevanje in certificiranje kibernetske varnosti kot mehanizem za zagotavljanje kakovosti v dobavni verigi. Ta sistem certificiranja bo usklajen s certifikacijskim okvirom EU za digitalne proizvode, storitve in postopke IKT, ki je bil vzpostavljen z Aktom EU o kibernetski varnosti (2019/881).

Izboljšanje kibernetske varnosti dobavne verige je zato izjemnega pomena. To je mogoče doseči z vzpostavitvijo močnih politik za spodbujanje MSP, z zagotavljanjem smernic za zahteve glede kibernetske varnosti v postopkih javnih naročil s strani javnih uprav, spodbujanjem sodelovanja v zasebnem sektorju, izgradnjo javno-zasebnih partnerstev, spodbujanjem mehanizmov za usklajeno razkrivanje šibkih točk (CVD)[18], razvojem certifikacijske sheme za produkte, vključno s komponentami kibernetske varnosti v digitalnih pobudah za MSP, ter s financiranjem razvoja znanj in spretnosti.

Varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve

Komisija je februarja 2020 v sporočilu z naslovom „Oblikovanje digitalne prihodnosti Evrope“[19] predstavila svojo vizijo digitalne preobrazbe EU, katere cilj je zagotoviti vključujočo tehnologijo, ki deluje za ljudi in spoštuje temeljne vrednote EU. Sporočilo zlasti navaja, da je spodbujanje digitalne preobrazbe javnih uprav po vsej Evropi ključnega pomena. V tem smislu je bistvenega pomena krepitev zaupanja v vlado v zvezi z digitalno identiteto in zaupanja v javne storitve. To je še toliko bolj pomembno, če upoštevamo dejstvo, da so transakcije in izmenjave podatkov v javnem sektorju pogosto občutljive narave.

Številne države so izrazile namero, da bodo to vprašanje obravnavale v svojih nacionalnih strategijah za kibernetsko varnost, kot na primer: Danska, Estonija, Francija, Luksemburg, Malta, Španija, Nizozemska in Združeno kraljestvo. Med temi državami so nekatere tudi navedle, da bi lahko ta strateški cilj obravnavali kot del širšega načrta:

- Estonija povezuje svoj akcijski načrt o „varnosti elektronske identitete in zmogljivosti elektronske avtentikacije“ s širšo digitalno agendo 2020 za Estonijo.
- Francoska nacionalna strategija za kibernetsko varnost navaja, da državni sekretar, pristojen za digitalno tehnologijo, nadzoruje pripravo načrta za „varovanje digitalnega življenja, zasebnosti in osebnih podatkov francoskega prebivalstva“.
- Nizozemska nacionalna strategija za kibernetsko varnost navaja, da so kibernetska varnost v javnih upravah ter javne storitve, ki se zagotavljajo državljanom in podjetjem, podrobneje obravnavane v širši agendi za digitalno upravo.
- Vlada Združenega kraljestva seli vse več svojih storitev na splet, zato je imenovala posebno vladno digitalno službo (GDS), da bi zagotovila, da so vse nove digitalne

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

storitve, ki jih ustvari ali naroči vlada, tudi „privzeto varne“, pri čemer jo podpira britanski nacionalni center za kibernetsko varnost (NCSC).

2.2.3 Drugi obravnavani strateški cilji

V fazi teoretičnih raziskav in kot del razgovorov, ki jih je opravila agencija ENISA, so bili preučeni tudi drugi strateški cilji. Vendar je bila sprejeta odločitev, da ti cilji ne bodo del okvirja za samoocenjevanje.

V PRILOGI C – Drugi preučeni cilji so opisane opredelitve za vsakega od teh ciljev, ki se lahko uporabijo za spodbujanje prihodnjih razprav o možnih izboljšavah na področju nacionalne strategije za kibernetsko varnost.

Za razmislek v prihodnosti so bili proučeni naslednji strateški cilji:

- razvoj strategij kibernetske varnosti za posamezne sektorje;
- boj proti dezinformacijskim kampanjam;
- varne najsodobnejše tehnologije (5G, umetna inteligenca, kvantno računalništvo ...);
- zagotavljanje podatkovne suverenosti in
- zagotavljanje spodbud za razvoj industrije kibernetskega zavarovanja.

2.3 KLJUČNI IZVLEČKI IZ PRIMERJALNE ANALIZE

Namen teoretične raziskave o obstoječih zrelostnih modelih, povezanih s kibernetsko varnostjo, je bil zbrati informacije in dokaze, da bi podprli oblikovanje okvirja za samoocenjevanje nacionalnih zmogljivosti na področju nacionalne strategije za kibernetsko varnost. V zvezi s tem je bil opravljen obsežen pregled literature o obstoječih modelih, da bi dopolnili ugotovitve iz začetne raziskave o določitvi obsega modelov zrelosti kibernetske varnosti in obstoječe nacionalne strategije za kibernetsko varnost, ki so predstavljene v poglavjih 2.1 in 2.2. Sistematični pregled lahko služi v oporo pri izbiri in utemeljitvi ravni zrelosti ocenjevalnega okvirja ter za opredelitev različnih razsežnosti in kazalnikov.

V okviru sistematičnega pregleda zrelostnih modelov je bilo obravnavanih in analiziranih 10 modelov, in sicer na podlagi njihovih ključnih značilnosti. Splošni pregled ključnih značilnosti vsakega pregledanega modela v okviru te študije je na voljo v Preglednici 2: Pregled analiziranih zrelostnih modelov, podrobnejša analiza pa je na voljo v PRILOGI A.

Preglednica 2: Pregled analiziranih zrelostnih modelov

Ime modela	# ravni zrelosti	# atributov	Metoda ocenjevanja	Prikaz rezultatov
Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM)	5	5 glavnih razsežnosti	sodelovanje z lokalno organizacijo za izpopolnitev modela pred njegovo uporabo v nacionalnem okviru	polarni (radarski) grafikon s 5 razdelki
Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2)	4	10 glavnih področij	metodologija in nabor orodij za samoocenjevanje	preglednica rezultatov s tortnimi grafikoni
Okvir za izboljšanje kibernetske varnosti kritične infrastrukture	n. r. (4 stopnje)	5 osrednjih funkcij	Samoocenjevanje	N. r.
Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2)	5	5 glavnih področij	n. r.	n. r.

Certificiranje zrelosti na področju kibernetske varnosti (CMMC)	5	17 glavnih področij	ocena s strani neodvisnih revizorjev	n. r.
Zrelostni model kibernetske varnosti skupnosti (CCSMM)	5	6 glavnih razsežnosti	ocenjevanje v skupnostih ob sodelovanju državnih in zveznih organov kazenskega pregona	n. r.
Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (ISMM)	5	23 ocenjenih področij	n. r.	n. r.
Model službe za notranjo revizijo za javni sektor (IA-CM)	5	6 elementov	samoocenjevanje	n. r.
Svetovni indeks kibernetske varnosti (GCI)	n. r.	5 stebrov	samoocenjevanje	tabela z razvrstitvijo
Indeks kibernetske moči (CPI)	n. r.	4 kategorije	primerjalna analiza, ki jo opravi podjetje Economist Intelligence Unit	tabela z razvrstitvijo

Ta sistematični pregled je omogočil oblikovanje zaključkov o najboljših praksah, sprejetih v obstoječih modelih, ter tako nudil podporo za razvoj konceptualnega modela za trenutni zrelostni model. Primerjalna analiza je predstavljala predvsem oporo za opredelitev ravni zrelosti, oblikovanje sklopov razsežnosti in izbiro kazalnikov ter ustrezno metodologijo vizualizacije rezultatov modela. Najpomembnejše ugotovitve za vsakega od teh elementov so podrobno opisane v Preglednici 3.

Preglednica 3: Ključni izvlečki iz primerjalne analize

Značilnost	Ključni izvlečki
Ravni zrelosti	▶ Petstopenjska lestvica zrelosti za okvire ocenjevanja na področju zmogljivosti kibernetske varnosti je splošno sprejeta in lahko zagotovi razčlenjene rezultate ocenjevanja (za izčrpen pregled opredelitve ravni zrelosti za posamezni model glej Preglednico 6 Primerjava ravni zrelosti). ▶ Vsi modeli zagotavljajo visoko raven opredelitve za posamezno raven zrelosti, ki se nato prilagodi različnim razsežnostim ali sklopom razsežnosti. ▶ Pri merjenju zrelosti na področju zmogljivosti kibernetske varnosti se običajno ocenita dva glavna vidika: zrelost strategij in zrelost postopkov, vzpostavljenih za izvajanje strategij.
Atributi	▶ Primerjalna analiza atributov obstoječih modelov zrelosti kaže heterogene rezultate, kjer je povprečno število atributov na model med štiri in pet. ▶ Model, ki temelji na približno štirih ali petih atributih, državam zagotavlja ustrezno raven razčlenjenosti podatkov, tako da združuje ustrezne razsežnosti in zagotavlja berljivost rezultatov (za opis atributov za posamezni model glej Preglednico 7: Primerjava lastnosti/razsežnosti). ▶ Ključno načelo, ki je bilo pri opredelitvi sklopov sprejeto v vseh modelih, temelji na skladnosti elementov, razvrščenih v posamezne sklope.
Metoda presoje	▶ Metode ocenjevanja, uporabljene v različnih analiziranih modelih, se med seboj razlikujejo. ▶ Najpogostejša metoda ocenjevanja temelji na samoocenjevanju.
Prikaz rezultatov	▶ Pomembno je, da so rezultati predstavljeni na različnih ravneh razčlenjenosti. ▶ Metodologija vizualizacije mora biti razumljiva in lahko berljiva.

Konceptualni model je temeljil na primerjalni analizi različnih zrelostnih modelov in na predhodnem delu agencije ENISA. Odločeno je bilo tudi, da se nadgradi *spletno interaktivno orodje agencije ENISA*, da bi razvili kazalnike zrelosti, ki se uporabljajo za posamezni atribut.

2.4 IZZIVI PRI OCENJEVANJU NACIONALNE STRATEGIJE ZA KIBERNETSKO VARNOST

Države članice se soočajo s številnimi izzivi pri krepitvi zmogljivosti na področju kibernetske varnosti, natančneje pri zagotavljanju, da so njihove zmogljivosti posodobljene v skladu z najnovejšimi spremembami. V nadaljevanju je povzetek izzivov, ki so jih države članice opredelile in o njih razpravljale v okviru te študije:

- **Težave pri usklajevanju in sodelovanju:** usklajevanje prizadevanj na področju kibernetske varnosti na nacionalni ravni, da bi se učinkovito odzivali na vprašanja kibernetske varnosti, se lahko izkaže za izziv zaradi velikega števila vključenih deležnikov.
- **Pomanjkanje virov za izvajanje ocenjevanja:** glede na lokalne razmere in strukturo nacionalnega upravljanja na področju kibernetske varnosti lahko ocenjevanje nacionalne strategije za kibernetsko varnost in njenih ciljev traja do 15 delovnih dni na osebo ali še dlje.
- **Pomanjkanje podpore za razvoj zmogljivosti na področju kibernetske varnosti:** nekatere države članice so se strinjale, da morajo za zaščito proračuna in pridobitev podpore za razvoj zmogljivosti na področju kibernetske varnosti najprej izvesti fazo ocenjevanja, da bi opredelile vrzeli in omejitve.
- **Težave pri dodeljevanju uspehov ali sprememb strategiji:** ker se grožnje razvijajo vsak dan in se tehnologija izboljšuje, je treba akcijske načrte nenehno prilagajati. Vendar pa ocenjevanje nacionalne strategije za kibernetsko varnost in dodeljevanje

sprememb sami strategiji ostaja težavna naloga. Zaradi tega je težko opredeliti omejitve in pomanjkljivosti nacionalne strategije za kibernetsko varnost.

- **Težave pri merjenju učinkovitosti nacionalne strategije za kibernetsko varnost:** za merjenje različnih področij, kot so napredek, izvajanje, zrelost in učinkovitost, se lahko zberejo metrike. Čeprav je merjenje napredka in izvajanja razmeroma enostavno v primerjavi z merjenjem učinkovitosti, je slednje še vedno bolj smiselno za ocenjevanje rezultatov in učinkov nacionalne strategije za kibernetsko varnost. Na podlagi razgovorov, ki jih je opravila agencija ENISA, je veliko število držav članic navedlo, da je kvantitativno merjenje učinkovitosti nacionalne strategije za kibernetsko varnost pomembno, vendar je tudi zelo zahtevna naloga, ki je v nekaterih primerih precej nemogoča.
- **Težave pri sprejemanju skupnega okvirja:** države članice EU delujejo v različnih kontekstih, kar zadeva politiko, organizacije, kulturo, družbeno strukturo in zrelost nacionalne strategije za kibernetsko varnost. Nekatere države članice, s katerimi so bili opravljeni razgovori v okviru te študije, so izjavile, da bi se lahko izkazalo, da je težko braniti in uporabljati enoten okvir za samoocenjevanje, ki bi ustrezal vsem.

2.5 KORISTI OCENJEVANJA NACIONALNIH ZMOGLJIVOSTI

Od leta 2017 imajo vse države članice EU nacionalno strategijo za kibernetsko varnost[20]. Čeprav je to spodbudno, je pomembno tudi, da so države članice sposobne ustrezno oceniti svoje nacionalne strategije za kibernetsko varnost ter tako zagotoviti dodano vrednost njihovemu strateškemu načrtovanju in izvajanju.

Eden od ciljev okvirja za ocenjevanje nacionalnih zmogljivosti je oceniti zmogljivosti kibernetske varnosti na podlagi prednostnih nalog, določenih v različnih nacionalnih strategijah za kibernetsko varnost. V okviru se pravzaprav ocenjuje raven zrelosti držav članic na področju zmogljivosti kibernetske varnosti na področjih, opredeljenih v ciljih nacionalne strategije za kibernetsko varnost. Rezultati okvira tako oblikovalcem politik držav članic pomagajo pri opredelitvi nacionalne strategije za kibernetsko varnost, saj jim zagotavljajo informacije o trenutnem stanju[21]. Cilj okvira NCAF je državam članicam pomagati pri opredelitvi področij, na katerih so potrebne izboljšave, in vzpostavitvi zmogljivosti.

Namen okvirja je državam članicam pomagati pri samoocenjevanju njihove ravni zrelosti z ocenjevanjem ciljev njihovih nacionalnih strategij za kibernetsko varnost, kar jim bo v pomoč pri krepitvi in razvoju zmogljivosti na področju kibernetske varnosti tako na strateški kot operativni ravni.

V praktičnem smislu so bile na podlagi razgovorov, ki jih je agencija ENISA opravila z več agencijami, odgovornimi za področje kibernetske varnosti v različnih državah članicah, opredeljene in poudarjene naslednje koristi okvirja za ocenjevanje nacionalnih zmogljivosti:

- zagotavljanje koristnih informacij za razvoj dolgoročne strategije (npr. dobre prakse, smernice);
- pomoč pri prepoznavanju manjkajočih elementov v nacionalni strategiji za kibernetsko varnost;
- pomoč pri nadaljnji krepitvi zmogljivosti na področju kibernetske varnosti;
- podpora pri sprejemanju odgovornosti v zvezi s političnimi ukrepi;
- zagotavljanje verodostojnosti pred širšo javnostjo in mednarodnimi partnerji;

[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.

- podpora pri ozaveščanju in izboljšanju javne podobe organizacije kot pregledne organizacije;
- pomoč pri predvidevanju prihodnjih problematik;
- pomoč pri opredelitvi pridobljenih izkušenj in dobrih praks;
- zagotavljanje skupnega izhodišča na področju zmogljivosti kibernetske varnosti po vsej EU z namenom olajšanja razprav in
- pomoč pri ocenjevanju nacionalnih zmogljivosti na področju kibernetske varnosti.

3. KAZALNIKI OKVIRA ZA OCENJEVANJE NACIONALNIH ZMOGLJIVOSTI

3.1 SPLOŠNI NAMEN

Glavni cilj okvira NCAF je izmeriti raven zrelosti zmogljivosti **držav članic** na področju kibernetske varnosti, da se jim pomaga pri ocenjevanju njihovih nacionalnih zmogljivosti na področju kibernetske varnosti, krepitvi ozaveščenosti o ravni zrelosti države, opredelitvi področij, ki jih je treba izboljšati, in krepitvi zmogljivosti na področju kibernetske varnosti.

3.2 RAVNI ZRELOSTI

Okvir temelji na **petih ravneh zrelosti**, ki opredeljujejo faze, ki jih države članice izvajajo pri krepitvi zmogljivosti kibernetske varnosti na področju, zajetem v posameznem cilju nacionalne strategije za kibernetsko varnost. Ravni predstavljajo naraščajoče ravni zrelosti. Prva je začetna **raven 1**, na kateri države članice nimajo jasno opredeljenega pristopa za razvoj zmogljivosti na področju kibernetske varnosti na področjih, ki jih zajemajo cilji nacionalne strategije za kibernetsko varnost, zadnja pa **raven 5**, na kateri je strategija za razvoj zmogljivosti na področju kibernetske varnosti dinamična in se prilagaja dogodkom v okolju. Preglednica 4 prikazuje lestvico ravni zrelosti in opis posamezne ravni.

Preglednica 4: Petstopenjska lestvica zrelosti okvirja agencije ENISA za ocenjevanje nacionalnih zmogljivosti

RAVEN 1 – ZAČETNA/AD HOC	RAVEN 2 – ZGODNJA OPREDELITEV	RAVEN 3 – VZPOSTAVLJENOST	RAVEN 4 – OPTIMIZACIJA	RAVEN 5 – PRILAGODLJIVOST
Država članica nima jasno opredeljenega pristopa za razvoj zmogljivosti na področju kibernetske varnosti na področjih, ki jih zajemajo cilji nacionalne strategije za kibernetsko varnost. Kljub temu ima država morda vzpostavljene nekatere splošne cilje in je izvedla nekatere študije (tehnične, politične, usmeritvene) za izboljšanje nacionalnih zmogljivosti.	Opredeljen je bil nacionalni pristop za razvoj zmogljivosti na področjih, ki so zajeta v ciljih nacionalne strategije za kibernetsko varnost. Akcijski načrti ali aktivnosti za doseganje rezultatov so vzpostavljeni, vendar so še v zgodnji fazi. Poleg tega so bili morda opredeljeni in/ali vključeni aktivni deležniki.	Akcijski načrt za razvoj zmogljivosti na področjih, ki so zajeta v ciljih nacionalne strategije za kibernetsko varnost, je jasno opredeljen in ga podpirajo zadevni deležniki. Prakse in aktivnosti se izvršujejo in enotno izvajajo na nacionalni ravni. Aktivnosti so opredeljene in dokumentirane, imajo jasno začrtan način dodeljevanja sredstev in upravljanja ter določene roke.	Akcijski načrt se redno ocenjuje: ima določene prednostne naloge, je optimiziran in trajnosten. Uspešnost aktivnosti pri razvoju zmogljivosti na področju kibernetske varnosti se redno meri. Opredeljeni so dejavniki uspeha, izzivi in vrzeli pri izvajanju aktivnosti.	Strategija za razvoj zmogljivosti na področju kibernetske varnosti je dinamična in prilagodljiva. Stalna pozornost na dogodke/spremembe v okolju (tehnološki napredek, svetovni konflikti, nove grožnje ...) spodbuja sposobnost hitrega odločanja in sposobnost hitrega ukrepanja s ciljem izboljšanja.

3.3 SKLOPI IN KROVNA STRUKTURA OKVIRJA ZA SAMOOCENJEVANJE

Okvir za samoocenjevanje ima **štiri sklope**: (I) upravljanje in standardi kibernetske varnosti, (II) krepitev zmogljivosti in ozaveščanje, (III) pravo in regulativa ter (IV) sodelovanje. Vsak od teh sklopov zajema ključno tematsko področje za krepitev zmogljivosti kibernetske varnosti v državi in vsebuje nabor različnih ciljev, ki bi jih države članice lahko vključile v svojo nacionalno strategijo za kibernetsko varnost. Še zlasti:

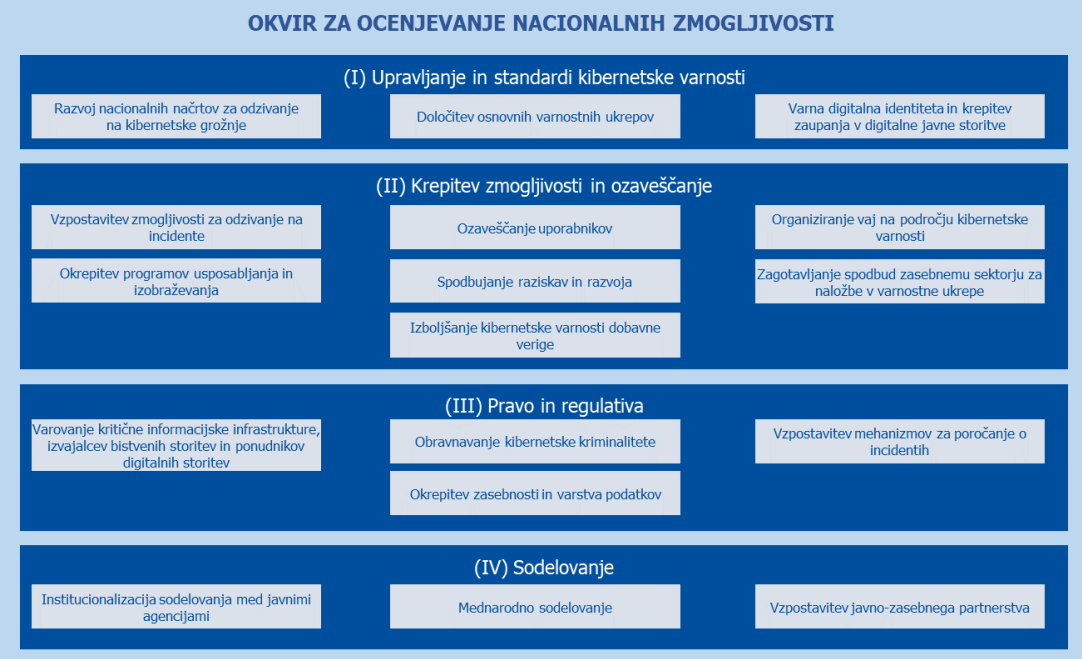
- **(I) Upravljanje in standardi kibernetske varnosti**: ta sklop meri zmogljivost držav članic za vzpostavitev ustreznega upravljanja, standardov in dobrih praks na področju kibernetske varnosti. Ta razsežnost upošteva različne vidike kibernetske obrambe in odpornosti, hkrati pa podpira razvoj nacionalne industrije na področju kibernetske varnosti in krepi zaupanje v vlade;
- **(II) Krepitev zmogljivosti in ozaveščanje**: ta sklop ocenjuje zmogljivost držav članic za ozaveščanje o tveganjih in grožnjah na področju kibernetske varnosti ter o tem, kako se spopasti z njimi. Poleg tega ta razsežnost meri sposobnost države, da stalno razvija zmogljivosti kibernetske varnosti ter povečuje splošno raven znanja in spretnosti na tem področju. Obravnava razvoj trga kibernetske varnosti in napredek v raziskavah in razvoju na področju kibernetske varnosti. Ta sklop prerazporeja vse cilje, ki postavljajo temelje za krepitev zmogljivosti;
- **(III) Pravo in regulativa**: ta sklop meri zmogljivost držav članic za vzpostavitev potrebnih pravnih in regulativnih instrumentov za obravnavanje in boj proti porastu kibernetske kriminalitete in povezanih kibernetskih incidentov ter za zaščito kritične informacijske infrastrukture. Poleg tega se s to razsežnostjo ocenjuje tudi zmogljivost držav članic, da oblikujejo pravni okvir za zaščito državljanov in podjetij, na primer uravnoteženje varnosti z zasebnostjo;
- **(IV) Sodelovanje**: ta sklop ocenjuje sodelovanje in izmenjavo informacij med različnimi skupinami deležnikov na nacionalni in mednarodni ravni kot pomembno orodje za boljše razumevanje nenehno spreminjajočega se nevarnega okolja in odzivanje nanj.

Cilji, ki so vključeni v model, so tisti, ki jih države članice običajno sprejmejo, in so bili izbrani med cilji, navedenimi v poglavju 2.2. V modelu so ocenjeni zlasti naslednji cilji:

- 1. razvoj nacionalnih načrtov za odzivanje na kibernetske grožnje (I);
- 2. določitev osnovnih varnostnih ukrepov (I);
- 3. varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve (I);
- 4. vzpostavitev zmogljivosti za odzivanje na incidente (II);
- 5. ozaveščanje uporabnikov (II);
- 6. organizacija vaj na področju kibernetske varnosti (II);
- 7. okrepitev programov usposabljanja in izobraževanja (II);
- 8. spodbujanje raziskav in razvoja (II);
- 9. zagotavljanje spodbud zasebnemu sektorju za naložbe v varnostne ukrepe (II);
- 10. izboljšanje kibernetske varnosti dobavne verige (II);
- 11. varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in ponudnikov digitalnih storitev (III);
- 12. obravnavanje kibernetske kriminalitete (III);
- 13. vzpostavitev mehanizmov za poročanje o incidentih (III);
- 14. okrepitev zasebnosti in varstva podatkov (III);
- 15. institucionalizacija sodelovanja med javnimi agencijam (IV);
- 16. mednarodno sodelovanje (IV);
- 17. vzpostavitev javno-zasebnega partnerstva (IV).

Štirje sklopi in osnovni cilji so združeni v model, da bi imeli celovit pregled nad zrelostjo zmogljivosti držav članic na področju kibernetske varnosti. Slika 1 predstavlja krovno strukturo okvirja za samoocenjevanje in prikazuje, kako so ti elementi, tj. cilji, sklopi in okvir za samoocenjevanje, povezani z ocenjevanjem uspešnosti države.

Slika 1: Struktura okvirja za samoocenjevanje



Za vsak cilj, vključen v okvir za samoocenjevanje, obstaja vrsta kazalnikov, ki so porazdeljeni med pet ravni zrelosti. Vsak kazalnik temelji na dihotomnem vprašanju (da/ne). Kazalnik je lahko potreben/nujen ali neobvezen.

3.4 MEHANIZEM TOČKOVANJA

Mehanizem točkovanja okvirja za samoocenjevanje upošteva zgoraj navedene elemente in načela iz poglavja 3.5. Model zagotavlja oceno, ki temelji na vrednosti dveh parametrov, **ravni zrelosti** in **deležu pokritosti**. Vsak od teh parametrov se lahko izračuna na različnih ravneh: (i) po ciljih, (ii) po sklopu ciljev ali (iii) na skupni ravni.

Ocene na ravni ciljev

Ocena ravni zrelosti zagotavlja pregled ravni zrelosti, tako da prikazuje, katere zmogljivosti in prakse so bile vzpostavljene. Ocena ravni zrelosti se izračuna kot najvišja raven, za katero je respondent izpolnil vse zahteve (*tj.* odgovor DA na vsa obvezna vprašanja), poleg tega pa je izpolnil vse zahteve iz prejšnjih ravni zrelosti.

Delež pokritosti kaže obseg pokritosti vseh kazalnikov, pri katerih je odgovor pritrdilen, ne glede na njihovo raven. Gre za dopolnilno vrednost, ki upošteva vse kazalnike, ki merijo cilj. Delež pokritosti se izračuna kot razmerje med skupnim številom vprašanj v okviru cilja in številom vprašanj, za katera je odgovor pritrdilen.

Pomembno je pojasniti, da se v preostalem dokumentu beseda ***ocena*** uporablja za sklicevanje tako na vrednosti ravni zrelosti kot na delež pokritosti.

Slika 2 – Mehanizem točkovanja po ciljih zagotavlja vizualizacijo ocenjevalnega mehanizma, opisanega v poglavju 3.1, ki bo nadalje razvit v nadaljevanju.

Slika 2: Mehanizem točkovanja po ciljih

Slika 2 prikazuje primer, kako se raven zrelosti izračuna glede na cilj. Omeniti je treba, da je respondent izpolnil vse zahteve prvih treh ravni zrelosti in le delno izpolnil zahteve ravni 4. Zato ocena kaže, da je ***raven zrelosti respondenta za cilj „organiziranje vaje na področju kibernetske varnosti“ raven 3****.*

Vendar v primeru, prikazanem na Sliki 2, raven zrelosti cilja ne more zajeti informacij, ki jih zagotavljajo kazalniki, ki imajo pozitiven rezultat in so nad 3. ravnjo zrelosti. V tem primeru lahko delež pokritosti zagotovi pregled vseh elementov, ki jih je respondent izvedel za dosego tega cilja, kljub dejanski ravni zrelosti. V tem primeru je razmerje med skupnim številom vprašanj v okviru cilja in številom vprašanj, pri katerih je odgovor pritrdilen, enako 19/27, tj. ***vrednost deleža pokritosti je 70 %****.*

Da bi se prilagodili posebnostim držav članic in hkrati omogočili dosleden pregled, se ocena izračuna na podlagi dveh različnih vzorcev na ravni sklopov in na skupni ravni:

- **Splošne ocene**: en popoln vzorec, ki zajema vse cilje znotraj sklopa ali znotraj celotnega okvirja (od prvega do 17. cilja);
- **Specifične ocene**: en specifičen vzorec, ki zajema samo cilje, ki jih izbere država članica (običajno ustreza ciljem, ki so prisotni v nacionalni strategiji za kibernetsko varnost določene države) znotraj sklopa ali znotraj celotnega okvirja.

Ocene na ravni sklopov

Splošna raven zrelosti posameznega sklopa se izračuna kot aritmetična sredina ravni zrelosti vseh ciljev znotraj tega sklopa.

Specifična raven zrelosti posameznega sklopa se izračuna kot aritmetična sredina ravni zrelosti ciljev znotraj tega sklopa, ki jih je država članica izbrala za ocenjevanje (običajno ustrezajo ciljem, ki so prisotni v nacionalni strategiji za kibernetsko varnost določene države).

Slika 1 kaže na primer, da je sklop (1) upravljanje in standardi kibernetske varnosti sestavljen iz treh ciljev. Ob predpostavki, da se je respondent odločil oceniti samo prva dva cilja, ne pa tudi

tretjega, in ob predpostavki, da prva dva cilja predstavljata raven zrelosti 2 oziroma 4, je raven zrelosti sklopa ob upoštevanju vseh ciljev raven 2 (sklop (I) splošna raven zrelosti = (2+4)/3), medtem ko je raven zrelosti sklopa, kjer se upoštevajo le specifični cilji, ki jih izbere ocenjevalec, raven 3 (sklop (I) specifična raven zrelosti = (2+4)/2).

Splošni delež pokritosti posameznega sklopa se izračuna kot razmerje med skupnim številom vprašanj v okviru sklopa in številom vprašanj, za katera je odgovor pritrdilen.

Specifični delež pokritosti posameznega sklopa se izračuna kot razmerje med skupnim številom vprašanj znotraj sklopa, ki se nanašajo na cilje, ki jih je država članica izbrala za ocenjevanje (običajno ustrezajo ciljem iz nacionalne strategije za kibernetsko varnost določene države), in številom vprašanj, za katera je odgovor pritrdilen.

Ocene na skupni ravni

Skupna splošna raven zrelosti države se izračuna kot aritmetična sredina ravni zrelosti vseh ciljev znotraj okvirja, od prvega do 17. cilja.

Skupna specifična raven zrelosti države se izračuna kot aritmetična sredina ravni zrelosti ciljev znotraj okvirja, ki jih je država članica izbrala za ocenjevanje (običajno ustrezajo ciljem, ki so prisotni v nacionalni strategiji za kibernetsko varnost določene države).

Skupni splošni delež pokritosti države se izračuna kot razmerje med skupnim številom vprašanj v okviru vseh ciljev, vključenih v okvir (od prvega do 17.), in številom vprašanj, za katera je odgovor pritrdilen.

Skupni specifični delež pokritosti države se izračuna kot razmerje med skupnim številom vprašanj v okviru ciljev, vključenih v okvir, ki jih je država članica izbrala za ocenjevanje (običajno ustrezajo ciljem iz nacionalne strategije za kibernetsko varnost določene države), in številom vprašanj, za katera je odgovor pritrdilen.

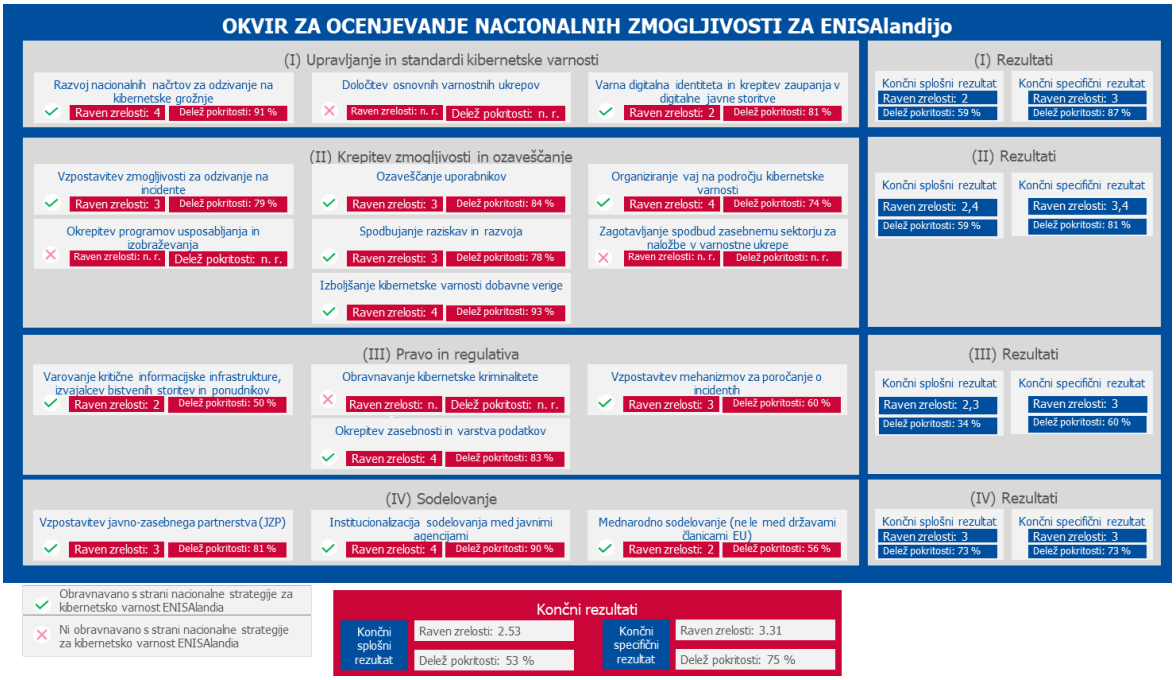
Respondenti lahko za vsak kazalnik kot svoj odgovor izberejo tretjo možnost „ne vem/ni relevantno“. V tem primeru se kazalnik izključi iz skupnega izračuna rezultatov.

Ravni zrelosti na ravni sklopov in na skupni ravni se izračunajo z aritmetično sredino, da se prikaže napredek med dvema ocenama. Dejansko druga možnost, ki vključuje izračun zrelosti na ravni sklopov in na skupni ravni kot raven zrelosti najmanj zrelega cilja – čeprav je z vidika zrelosti pomembna –, ne more upoštevati napredka, doseženega na področjih, ki jih zajemajo drugi cilji.

Ker se raven sklopov in skupna raven konsolidirata za namene poročanja, je bila sprejeta odločitev, da se uporabi aritmetična sredina. Za večjo natančnost pri poročanju uporabite ocene na ravni ciljev.

Na sliki 3 spodaj so povzeti mehanizmi točkovanja na različnih ravneh modela (cilj, sklop, skupaj).

Slika 3: Mehanizem skupnega točkovanja



3.5 ZAHTEVE ZA OKVIR SAMOOCENJEVANJA

Okvir za ocenjevanje nacionalnih zmogljivosti (okvir NCAF), predstavljen v tem poglavju, temelji na potrebah, ki so jih poudarile države članice, in je zgrajen na nizu zahtev, navedenih v nadaljevanju:

- država članica prostovoljno uporablja okvir NCAF kot okvir za samoocenjevanje;
- okvir NCAF je namenjen merjenju zmogljivosti držav članic na področju kibernetske varnosti, in sicer v povezavi s 17 cilji. Vendar pa lahko država članica izbere cilje, ki jih želi oceniti, in tako oceni le podskupino teh 17 ciljev;
- namen okvira za samoocenjevanje je merjenje ravni zrelosti države članice na področju zmogljivosti kibernetske varnosti;
- rezultati ocenjevanja se ne objavijo, razen če se država članica odloči, da bo to storila na lastno pobudo;
- država članica lahko rezultate ocenjevanja prikaže tako, da predstavi raven zrelosti države na področju zmogljivosti kibernetske varnosti, sklopa ciljev ali celo enega samega cilja;
- vsi ocenjeni cilji v ocenjevalnem okviru so enako pomembni. Enako velja za kazalnike, uporabljene znotraj okvira;
- država članica lahko spremlja napredek v daljšem časovnem obdobju.

Okvir za samoocenjevanje je namenjen podpori državam članicam pri krepitvi zmogljivosti na področju kibernetske varnosti. Zato vključuje tudi sklop priporočil ali smernic za usmerjanje evropskih držav pri izboljšanju njihove ravni zrelosti.

Opomba: ta priporočila ali smernice so splošna in temeljijo na publikacijah agencije ENISA in izkušnjah, pridobljenih v drugih državah, ter bodo temeljila na rezultatih samoocene.

4. KAZALNIKI OKVIRA ZA OCENJEVANJE NACIONALNIH ZMOGLJIVOSTI

4.1 KAZALNIKI OKVIRA

V tem poglavju so predstavljeni kazalniki okvira agencije ENISA za ocenjevanje nacionalnih zmogljivosti. Naslednja poglavja so razporejena po sklopih.

V vsakem sklopu je preglednica, v kateri je predstavljen obsežen nabor kazalnikov v obliki vprašanj, ki predstavljajo določeno raven zrelosti. Vprašalnik je glavni instrument za samoocenjevanje. Za vsak cilj sta dva sklopa kazalnikov, na katera je treba opozoriti:

- sklop splošnih vprašanj o zrelosti strategije (9 splošnih vprašanj), ki so označena s črkami od „a“ do „c“ za vsako raven zrelosti in se ponovijo za vsak cilj;
- sklop vprašanj glede zmogljivosti kibernetske varnosti (319 vprašanj glede zmogljivosti kibernetske varnosti), oštevilčenih od „1“ do „10“ za vsako raven zrelosti, ki je značilna za področje, ki ga zajema cilj.

Vsako vprašanje ima dodano oznako (0-1), ki kaže, ali je vprašanje potreben/nujen kazalnik (1) ali neobvezen kazalnik (0) za raven zrelosti.

Vsako vprašanje je mogoče opredeliti z identifikacijsko številko, ki jo sestavljajo:

- številka cilja,
- raven zrelosti in
- številka vprašanja.

Na primer, vprašanje z oznako ID 1.2.4 je četrto vprašanje na ravni zrelosti 2 znotraj strateškega cilja (I) „Razvoj nacionalnih načrtov za odzivanje na kibernetske grožnje“.

Opozoriti je treba, da se vprašanja v vprašalniku nanašajo na nacionalno raven, razen če je navedeno drugače. V vseh vprašanjih se zaimek „vi“ nanaša na državo članico v splošnem smislu in ne na posameznika ali vladni organ, ki izvaja ocenjevanje.

Opredelitev posameznih ciljev lahko najdete v poglavju 2.2 – Skupni cilji, opredeljeni v okviru evropskih nacionalnih strategij za kibernetsko varnost.

4.1.1 Sklop 1: Upravljanje in standardi kibernetske varnosti

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
1 – Razvoj nacionalnih načrtov za odzivanje na kibernetske grožnje	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste začeli pripravljati nacionalne načrte za odzivanje na kibernetske grožnje? *Npr.* določitev splošnih ciljev, področij uporabe in/ali načel načrtov za odzivanje na kibernetske grožnje ...	1	Ali imate doktrino/nacionalno strategijo, ki vključuje kibernetsko varnost kot dejavnik krize (tj. načrt, politika itd.)?	1	Ali imate nacionalni načrt za krizno upravljanje na področju kibernetske varnosti?	1	Ali ste zadovoljni s številom ali odstotkom ključnih sektorjev, vključenih v nacionalni načrt za odzivanje na kibernetske grožnje?	1	Ali imate vzpostavljen postopek pridobivanja izkušenj, ki sledi vajam iz kibernetske varnosti ali dejanskim krizam na nacionalni ravni?	1
	2	Ali se na splošno razume, da kibernetski incidenti predstavljajo krizni dejavnik, ki bi lahko ogrozil nacionalno varnost?	0	Ali imate vozlišče za pridobivanje informacij in obveščanje nosilcev odločanja? *Tj.* kakršnekoli metode, platforme ali lokacije za zagotovitev, da imajo vsi akterji kriznega odzivanja dostop do enakih informacij o kibernetski krizi v realnem času?	1	Ali imate vzpostavljene nacionalne postopke za kibernetske krize?	1	Ali dovolj pogosto organizirate dejavnosti (tj. vaje), povezane z nacionalnim načrtovanjem odzivanja na kibernetske grožnje?	1	Ali imate postopek za redno preizkušanje nacionalnega načrta?	1
	3	Ali so bile izvedene študije (tehnične, operativne, politične) na področju načrtovanja odzivanja na kibernetske grožnje?	0	Ali so na voljo ustrezni viri za nadzor razvoja in izvajanja nacionalnih načrtov za odzivanje na kibernetske grožnje?	1	Ali imate skupino za komuniciranje, ki je posebej usposobljena za odzivanje na kibernetske krize in obveščanje javnosti?	1	Ali imate dovolj ljudi, ki se ukvarjajo s kriznim načrtovanjem, proučevanjem pridobljenih izkušenj in izvajanjem sprememb?	1	Ali imate ustrezna orodja in platforme za ozaveščanje o razmerah?	1
	4	-		Ali imate metodologijo za ocenjevanje kibernetskih groženj na nacionalni ravni, ki vključuje postopke za oceno učinka?	0	Ali sodelujete z vsemi ustreznimi nacionalnimi deležniki (nacionalna varnost, obramba, civilna zaščita, kazenski pregon, ministrstva, organi itd.)?	1	Ali imate dovolj ljudi, usposobljenih za odzivanje na kibernetske krize na nacionalni ravni?	1	Ali uporabljate poseben model zrelosti za spremljanje in izboljšanje načrta za odzivanje na kibernetske grožnje?	0
	5	-		-		Ali imate ustrezne zmogljivosti za krizno upravljanje in situacijske sobe?	1	-		Ali imate vire, ki so specializirani za predvidevanje groženj ali delajo na področju kibernetske varnosti v prihodnosti, da bi zmogli reševati prihodnje krize ali prihodnje izzive?	0

	6	-		-	Ali sodelujete z mednarodnimi deležniki v EU, če je to potrebno?	0	-		-		
	7	-		-	Ali sodelujete z mednarodnimi deležniki iz držav nečlanic EU, če je to potrebno?	0	-		-		
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
2 – Določitev osnovnih varnostnih ukrepov	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste izvedli študijo, da bi opredelili zahteve in vrzeli za **javne** organizacije na podlagi mednarodno priznanih standardov? *Npr.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS ...	1	Ali so varnostni ukrepi v skladu z mednarodnimi/nacionalnimi standardi?	1	Ali so osnovni varnostni ukrepi obvezni?	1	Ali obstaja postopek za pogosto posodabljanje osnovnih varnostnih ukrepov?	1	Ali imate vzpostavljen postopek za utrjevanje varnosti IKT, kadar incidentov ni mogoče obravnavati s pomočjo ukrepov?	1
	2	Ali ste izvedli študijo, da bi opredelili zahteve in vrzeli za **zasebne** organizacije na podlagi mednarodno priznanih standardov? *Npr.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS ...	1	Ali se pri opredelitvi osnovnih varnostnih ukrepov opravi posvetovanje z zasebnim sektorjem in drugimi deležniki?	1	Ali izvajate horizontalne varnostne ukrepe v ključnih sektorjih?	1	Ali je vzpostavljen mehanizem spremljanja za preučevanje uporabe osnovnih varnostnih ukrepov?	1	Ali ocenjujete ustreznost novih standardov, ki so bili razviti kot odziv na najnovejši razvoj dogodkov v okolju groženj?	1
	3	-		-	Ali izvajate sektorske varnostne ukrepe v ključnih sektorjih?	1	Ali obstaja nacionalni organ, ki preverja, ali se osnovni varnostni ukrepi izvajajo ali ne?	1	Ali imate oziroma spodbujate postopek usklajenega razkrivanja šibkih točk na nacionalni ravni?	1	

	4	-				Ali so osnovni varnostni ukrepi v skladu z ustreznimi shemami certificiranja?	1	Ali imate vzpostavljen postopek za prepoznavanje neskladnosti organizacij v določenem časovnem obdobju?	1	-	
	5	-		-		Ali imate vzpostavljen postopek samoocene tveganja za osnovne varnostne ukrepe?	1	Ali obstaja revizijski postopek, ki zagotavlja pravilno uporabo varnostnih ukrepov?	1	-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**R**
2 – Določitev osnovnih varnostnih ukrepov	6	-		-		Ali pregledujete obvezne osnovne varnostne ukrepe v postopku javnega naročanja vladnih organov?	0	Ali opredeljujete ali dejavno spodbujate sprejetje varnih standardov za razvoj kritičnih proizvodov IT/OT (medicinska oprema, povezana in avtonomna vozila, profesionalni radio, težka industrijska oprema...)?	0	-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
3 – Varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste izvedli študije ali analize vrzeli, da bi ugotovili, kaj je potrebno za zagotovitev varnih digitalnih javnih storitev državljanom in podjetjem?	1	Ali izvajate analize tveganja, da bi ugotovili profil tveganja sredstev ali storitev, preden jih prenesete v oblak, ali da bi začeli s projekti digitalne preobrazbe?	1	Ali pri vseh projektih e-uprave spodbujate metodologije za vgrajeno zasebnost?	1	Ali zbirate kazalnike o incidentih na področju kibernetske varnosti, ki vključujejo kršitve varnosti digitalnih javnih storitev?	1	Ali sodelujete v evropskih delovnih skupinah, da bi ohranili standarde in/ali oblikovali nove zahteve za elektronske storitve zaupanja (elektronski podpisi, elektronski žigi, storitve elektronske priporočene dostave, časovni žigi, avtentikacija spletišč)? *Npr.* ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU ...	1

	2	-		Ali imate strategijo za vzpostavitev ali spodbujanje varnih nacionalnih shem elektronske identifikacije (eID) za državljane in podjetja?	1	Ali v oblikovanje in zagotavljanje varnih digitalnih javnih storitev vključujete zasebne deležnike?	1	Ali ste uvedli vzajemno priznavanje sredstev elektronske identifikacije z drugimi državami članicami?	1	Ali dejavno sodelujete pri medsebojnih strokovnih pregledih v okviru priglasitve shem elektronske identifikacije Evropski komisiji?	1
	3	-		Ali imate strategijo za vzpostavitev ali spodbujanje varnih nacionalnih elektronskih storitev zaupanja (elektronskih podpisov, elektronskih žigov, storitev elektronske priporočene dostave, časovnih žigov, avtentikacije spletišč) za državljane in podjetja?	1	Ali izvajate minimalno varnostno osnovo za vse digitalne javne storitve?	1	-		-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
3 – Varna digitalna identiteta in krepitev zaupanja v digitalne javne storitve	4	-		Ali imate strategijo za vladni oblak (strategijo za računalništvo v oblaku, namenjeno vladi in javnim organom, kot so ministrstva, vladne agencije in javne uprave ...), ki upošteva možne vplive na varnost?	0	Ali so državljanom in podjetjem na voljo sheme elektronske identifikacije s srednjo ali visoko ravnjo zanesljivosti, kot so opredeljene v Prilogi k Uredbi (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu?	1	-		-	
	5	-		-		Ali imate digitalne javne storitve, ki zahtevajo sheme elektronske identifikacije s srednjo ali visoko ravnjo zanesljivosti, kot so opredeljene v Prilogi k Uredbi (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu?	1	-		-	
	6	-		-		Ali imate ponudnike storitev zaupanja za državljane in podjetja (elektronski podpisi, elektronski žigi, storitve elektronske priporočene dostave, časovni žigi, avtentikacija spletišč)?	1	-		-	
	7	-		-		Ali spodbujate sprejetje osnovnih varnostnih ukrepov za vse modele uporabe računalništva v oblaku (npr. zasebni, javni, hibridni IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Sklop 2: Krepitev zmogljivosti in ozaveščanje

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
4 – Vzpostavitev zmogljivosti za odzivanje na incidente	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali se neformalne zmogljivosti za odzivanje na incidente upravljajo v javnem in zasebnem sektorju ali med njima?	1	Ali imate vsaj eno uradno nacionalno skupino CSIRT?	1	Ali imate zmogljivosti za odzivanje na incidente za sektorje iz Priloge II k direktivi o varnosti omrežij in informacij?	1	Ali ste opredelili in spodbujali standardizirane prakse za postopke odzivanja na incidente in sheme razvrščanja incidentov?	1	Ali imate vzpostavljene mehanizme za zgodnje odkrivanje, prepoznavanje, preprečevanje, odzivanje in blaženje ranljivosti ničtega dne?	1
	2	-		Ali imajo vaše nacionalne skupine CSIRT jasno opredeljen obseg posredovanja? *Npr.* odvisno od ciljnega sektorja, vrste incidenta, učinkov	1	Ali v vaši državi obstaja mehanizem sodelovanja skupine CSIRT za odzivanje na incidente?	1	Ali ocenjujete svojo zmogljivost odzivanja na incidente, da bi zagotovili, da imate ustrezne vire in spretnosti za opravljanje nalog iz točke (2) Priloge I k direktivi o varnosti omrežij in informacij?	1	-	
	3	-		Ali imajo vaše nacionalne skupine CSIRT jasno opredeljene odnose z drugimi nacionalnimi deležniki v zvezi z nacionalnim okoljem kibernetske varnosti in prakso odzivanja na incidente (npr. organi kazenskega pregona, vojska, ponudniki internetnih storitev, nacionalni centri za kibernetsko varnost)?	0	Ali imajo vaše nacionalne skupine CSIRT zmogljivost odzivanja na incidente v skladu s Prilogo I k direktivi o varnosti omrežij in informacij? *Tj.* razpoložljivost, fizična varnost, neprekinjeno poslovanje, mednarodno sodelovanje, spremljanje incidentov, zmogljivosti za zgodnje opozarjanje in obveščanje, odzivanje na incidente, analizo tveganja in spremljanje razmer, sodelovanje z zasebnim sektorjem, standardne prakse ...	1	-		-	

	4	-			Ali obstaja mehanizem sodelovanja z drugimi sosednjimi državami v zvezi z incidenti?	1	-		-		
	5	-		-	Ali ste formalno opredelili jasne politike in postopke za obvladovanje incidentov?	1	-		-		
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
4 – Vzpostavitev zmogljivosti za odzivanje na incidente	6	-		-		Ali vaše nacionalne skupine CSIRT sodelujejo pri vajah na področju kibernetske varnosti na nacionalni in mednarodni ravni?	1	-		-	
	7	-		-		Ali so vaše nacionalne skupine CSIRT povezane s FIRST (Forum skupin za odzivanje na incidente in računalniško varnost)?	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
5 – Ozaveščanje uporabnikov	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali vlada, zasebni sektor ali splošni uporabniki v minimalnem obsegu prepoznavajo, da je treba povečati ozaveščenost o vprašanjih kibernetske varnosti in zasebnosti?	1	Ali ste opredelili posebno ciljno skupino za ozaveščanje uporabnikov? *Npr.* splošni uporabniki, mladi, poslovni uporabniki (ki jih je mogoče dodatno razčleniti: MSP, izvajalci bistvenih storitev, ponudniki digitalnih storitev itd.)	1	Ali ste pripravili komunikacijske načrte/strategijo za kampanje?	1	Ali pripravljate merila za ocenjevanje vaše kampanje v fazi načrtovanja?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da so kampanje ozaveščanja vedno primerne glede na tehnološki napredek, spremembe v okolju grožnj, pravne predpise in direktive o nacionalni varnosti?	1

	2	Ali javne agencije znotraj svoje organizacije izvajajo ad hoc kampanje ozaveščanja o kibernetski varnosti? Npr. po incidentu na področju kibernetske varnosti?	0	Ali pripravljate projektni načrt za ozaveščanje o vprašanjih varnosti informacij in zasebnosti?	1	Ali imate vzpostavljen postopek za ustvarjanje vsebin na vladni ravni?	1	Ali izvajate evalvacijo svojih kampanj po njihovi izvedbi?	1	Ali izvajate redne ocene ali študije, da bi izmerili spreminjanje odnosa ali vedenja v zvezi z vprašanji kibernetske varnosti in zasebnosti v zasebnem in javnem sektorju?	1
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
5 – Ozaveščanje uporabnikov	3	Ali javne agencije izvajajo ad hoc kampanje ozaveščanja širše javnosti o kibernetski varnosti? *Npr.* po incidentu na področju kibernetske varnosti.	0	Ali imate na voljo vire, ki jih je mogoče zlahka prepoznati (*npr.* enotni spletni portal, orodja za ozaveščanje), za uporabnike, ki se želijo izobraževati o vprašanjih kibernetske varnosti in zasebnosti?	1	Ali imate vzpostavljene mehanizme za opredelitev ciljnih področij za ozaveščanje (tj. poročilo o naravi groženj, nacionalno okolje groženj, mednarodno okolje groženj, povratne informacije nacionalnih centrov za kibernetsko kriminaliteto itd.)?	1	Ali imate vzpostavljene mehanizme za opredelitev najpomembnejših medijev ali komunikacijskih kanalov glede na ciljne skupine, da bi čim bolj povečali doseg in udejstvovanje? *Npr.* različne vrste digitalnih medijev, brošure, elektronska pošta, učno gradivo, plakati na obljudenih območjih, televizija, radio ...	1	Ali se posvetujete s strokovnjaki za vedenje ljudi, da bi svojo kampanjo prilagodili ciljni skupini?	1
	4	-		-		Ali povezujete deležnike s strokovnjaki in skupinami za komuniciranje, da bi ustvarili vsebino?	1			-	
	5	-		-		Ali vključite zasebni sektor v svoja prizadevanja za ozaveščanje, da bi promovirali in razširjali sporočila širšemu občinstvu?	1	-		-	
	6	-		-		Ali pripravljate posebne pobude za ozaveščanje za vodstvene delavce v javnem, zasebnem, akademskem ali civilnodružbenem sektorju?	1	-		-	
	7	-		-		Ali sodelujete v kampanjah agencije ENISA ob evropskem mesecu kibernetske varnosti (ECSM)?	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
6 – Organiziranje vaj na področju kibernetske varnosti	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1

6 – Organiziranje vaj na področju kibernetske varnosti	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali izvajate vaje za obvladovanje krize v drugih sektorjih (razen v sektorjih kibernetske varnosti) na nacionalni ali vseevropski ravni?	1	Ali imate program vaj na področju kibernetske varnosti na nacionalni ravni?	1	Ali vključujete vse povezane organe javne uprave? (tudi če je scenarij prilagojen posameznemu sektorju)	1	Ali pišete poročila po zaključku ukrepanja/evalvacijska poročila?	1	Ali imate zmogljivosti za analizo pridobljenih izkušenj na področju kibernetske varnosti (procesi poročanja, analize, blažitev)?	1
	2	Ali ste dodelili sredstva za zasnovo in načrtovanje vaj iz kriznega upravljanja?	1	Ali izvajate oziroma dajete prednost vajam za obvladovanje kibernetskih kriz na ključnih družbenih funkcijah in v kritični infrastrukturi?	1	Ali v načrtovanje in izvajanje vaj vključujete zasebni sektor?	1	Ali preskušate načrte in postopke na nacionalni ravni?	1	Ali imate uveljavljen postopek za vrednotenje pridobljenih izkušenj?	1
	3	-		Ali ste opredelili usklajevalni organ za nadzor zasnove in načrtovanja vaj na področju kibernetske varnosti (javna agencija, posvetovalni organ ...)?	0	Ali organizirate vaje za posamezne sektorje na nacionalni in/ali mednarodni ravni?	1	Ali sodelujete v vajah na področju kibernetske varnosti na vseevropski ravni?	1	Ali prilagajate scenarije vaj glede na najnovejši razvoj dogodkov (tehnološki napredek, svetovni konflikti, okolje groženj ...)?	1
	4	-		-		Ali organizirate vaje v vseh ključnih sektorjih, navedenih v Prilogi II k direktivi o varnosti omrežij in informacij?	1	-		Ali svoje postopke kriznega upravljanja usklajujete z drugimi državami članicami, da bi zagotovili učinkovito vseevropsko krizno upravljanje?	1
	5	-		-		Ali organizirate večsektorske in/ali medsektorske vaje na področju kibernetske varnosti?	1	-		Ali imate vzpostavljen mehanizem za hitro prilagoditev strategije, načrtov in postopkov na podlagi izkušenj, pridobljenih med vajami?	0
	6	-		-		Ali organizirate vaje na področju kibernetske varnosti, ki so specifične za različne ravni? (tehnična in operativna raven, raven postopka, raven odločanja, politična raven ...)	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	#	Level 1	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
7 – Okrepitev programov usposabljanja in izobraževanja	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali razmišljate o razvoju programov usposabljanja in izobraževanja na področju kibernetske varnosti?	1	Ali pripravljate tečaje, namenjene kibernetski varnosti?	1	Ali je v vaši državi zajeta kultura kibernetske varnosti v zgodnji fazi izobraževanja učencev? Na primer, ali obravnavate področje kibernetske varnosti v srednjih šolah?	1	Ali pozivate k akreditaciji ali certificiranju osebja v zasebnem in javnem sektorju?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da so programi usposabljanja in izobraževanja vedno primerni glede na sedanji in nastajajoči tehnološki napredek, spremembe v okolju groženj, pravne predpise in direktive o nacionalni varnosti?	1
	2	-		Ali univerze v vaši državi ponujajo doktorske študije na področju kibernetske varnosti kot neodvisno disciplino in ne kot predmet na področju računalništva?	1	Ali imate nacionalne raziskovalne laboratorije in izobraževalne ustanove, specializirane za kibernetsko varnost?	1	Ali je vaša država razvila programe usposabljanja ali mentorstva na področju kibernetske varnosti za podporo nacionalnim zagonskim podjetjem in MSP?	1	Ali ustanavljate akademske centre odličnosti na področju kibernetske varnosti, ki bodo delovali kot vozlišča za raziskave in izobraževanje?	1
	3	-		Ali nameravate učitelje ne glede na njihovo področje usposabljati o vprašanjih, povezanih z varnostjo informacij in zasebnostjo? *Npr.* na področju spletne varnosti, varstva osebnih podatkov, spletnega nadlegovanja.	1	Ali spodbujate/financirate namenske tečaje in načrte usposabljanja o kibernetski varnosti za zaposlene v agencijah za zaposlovanje držav članic?	1	Ali dejavno spodbujate, da se v visokošolskem izobraževanju dodajo tečaji informacijske varnosti ne le za študente računalništva, temveč tudi za katero koli drugo poklicno specializacijo? *Npr.* tečaje, prilagojene potrebam tega poklica?	1	Ali akademske ustanove sodelujejo v vodenju razprav na področju izobraževanja in raziskav na področju kibernetske varnosti na mednarodni ravni?	0
	4	-		-		Ali imate tečaje na področju kibernetske varnosti in/ali specializirane učne načrte za ravni od 5 do 8 evropskega ogrodja kvalifikacij?	1	Ali redno ocenjujete vrzel v znanju in spretnostih (primanjkljaj delavcev na področju kibernetske varnosti) na področju informacijske varnosti?	1	-	

	5	-		-		Ali spodbujate in/ali podpirate pobude za vključitev tečajev o varnosti interneta v osnovnošolsko in srednješolsko izobraževanje?	1	Ali spodbujate mreženje in izmenjavo informacij med akademskimi ustanovami na nacionalni in mednarodni ravni?	1		
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
7 - Okrepitev programov usposabljanja in izobraževanja	6	-		-		Ali financirate ali ponujate brezplačna osnovna usposabljanja na področju kibernetske varnosti za državljane?	0	Ali v kakršni koli obliki vključujete zasebni sektor v pobude za izobraževanje o kibernetski varnosti? *Npr.* oblikovanje in izvajanje tečajev, pripravništva, delovne prakse ...	1	-	
	7	-		-		Ali organizirate letne dogodke o informacijski varnosti (npr. hekersko tekmovanje ali hekatone)?	0	Ali izvajate mehanizme financiranja, da bi spodbudili nastajanje diplom s področja kibernetske varnosti? *Npr.* štipendije, zagotovljeno vajeništvo/pripravništvo, zajamčena delovna mesta v določeni panogi ali vloge v javnem sektorju.	0	-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
8 – Spodbujanje raziskav in razvoja	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						

	1	Ali ste izvedli študije ali analize za opredelitev prednostnih nalog raziskav in razvoja na področju kibernetske varnosti?	1	Ali imate postopek za opredelitev prednostnih nalog na področju raziskav in razvoja (npr. nastajajoče teme za odvračanje, zaščito, odkrivanje in prilagajanje novim vrstam kibernetskih napadov)?	1	Ali obstaja načrt za povezovanje pobud na področju raziskav in razvoja z realnim gospodarstvom?	1	Ali so pobude za kibernetsko varnost na področju raziskav in razvoja v skladu z ustreznimi strateškimi cilji, npr. enotni digitalni trg, program Obzorje 2020, digitalna Evropa, strategija EU za kibernetsko varnost?	1	Ali si na nacionalni ravni prizadevate za sodelovanje z mednarodnimi pobudami na področju raziskav in razvoja, povezanimi s kibernetsko varnostjo?	1
	2	-		Ali je zasebni sektor vključen v določanje prednostnih nalog na področju raziskav in razvoja?	1	Ali obstajajo nacionalni projekti, povezani s kibernetsko varnostjo?	1	Ali obstaja shema vrednotenja za pobude na področju raziskav in razvoja?	1	Ali so prednostne naloge na področju raziskav in razvoja usklajene s sedanjo ali prihodnjo ureditvijo (nacionalna raven)?	1
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
8 – Spodbujanje raziskav in razvoja	3	-		Ali akademski krogi sodelujejo pri določanju prednostnih nalog na področju raziskav in razvoja?	1	Ali imate lokalne/regionalne ekosisteme zagonskih podjetij in druge kanale za mreženje (npr. tehnološki parki, inovacijski grozdi, dogodki/platforme za mreženje) za spodbujanje inovacij (tudi za zagonska podjetja na področju kibernetske varnosti)?	1	Ali obstajajo sporazumi o sodelovanju z univerzami in drugimi raziskovalnimi ustanovami?	1	Ali sodelujete pri vodenju razprav o eni ali več najsodobnejših temah na področju raziskav in razvoja na mednarodni ravni?	0
	4	-		Ali obstajajo nacionalne pobude na področju raziskav in razvoja, povezane s kibernetsko varnostjo?	0	Ali obstajajo naložbe v raziskovalne in razvojne programe na področju kibernetske varnosti v akademskem in zasebnem sektorju?	1	Ali obstaja priznan institucionalni organ, ki nadzoruje dejavnosti raziskav in razvoja na področju kibernetske varnosti?	0	-	
	5	-		-		Ali imate katedre za industrijske raziskave na univerzah, da bi povezali raziskovalne teme in potrebe trga?	1	-		-	
	6	-		-		Ali imate namenske programe financiranja raziskav in razvoja na področju kibernetske varnosti?	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Level 1**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**

9 – Zagotavljanje spodbud zasebnemu sektorju za naložbe v varnostne ukrepe	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali obstaja industrijska politika ali politična volja za spodbujanje razvoja industrije kibernetske varnosti?	1	Ali je zasebni sektor vključen v oblikovanje spodbud?	1	Ali obstajajo gospodarske/regulativne ali druge vrste spodbud za spodbujanje naložb v kibernetsko varnost?	1	Ali obstajajo zasebni akterji, ki se odzivajo na spodbude z vlaganjem v varnostne ukrepe? *Npr.* vlagatelji, specializirani za kibernetsko varnost, in nespecializirani vlagatelji.	1	Ali se pobude osredotočajo na teme kibernetske varnosti glede na najnovejši razvoj groženj?	1
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
9 – Zagotavljanje spodbud zasebnemu sektorju za naložbe v varnostne ukrepe	2	-		Ali ste opredelili posebne teme na področju kibernetske varnosti, ki jih je treba nasloviti? *Npr.* kriptografija, zasebnost, nova oblika avtentikacije, UI za kibernetsko varnost ...	0	Ali zagotavljate podporo (npr. davčne spodbude) za zagonska podjetja in MSP na področju kibernetske varnosti?	1	Ali spodbujate zasebni sektor, da se osredotoči na varnost najsodobnejših tehnologij? *Npr.* 5G, umetna inteligenca, internet stvari, kvantno računalništvo ...	1	-	
	3	-		-		Ali zagotavljate davčne spodbude ali druge finančne spodbude za vlagatelje iz zasebnega sektorja v zagonska podjetja na področju kibernetske varnosti?	1	-		-	
	4	-		-		Ali omogočate lažji dostop zagonskim podjetjem in MSP na področju kibernetske varnosti v postopku javnega naročanja?	0	-		-	
	5	-		-		Ali so na voljo proračunska sredstva za spodbujanje zasebnega sektorja?	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
10 – Izboljšanje kibernetske varnosti dobavne verige	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste izvedli študijo o dobrih praksah varnosti za upravljanje dobavne verige, ki se uporabljajo pri nabavi v različnih industrijskih segmentih in/ali javnem sektorju?	1	Ali izvajate ocene kibernetske varnosti v celotni dobavni verigi storitev in izdelkov IKT v ključnih sektorjih (kot je opredeljeno v Prilogi II direktive o varnosti omrežij in informacij (2016/1148))?	1	Ali uporabljate sisteme varnostnega certificiranja za izdelke in storitve, ki temeljijo na IKT? *Npr.* SOG-IS MRA v Evropi (odbora visokih uradnikov za varnost informacijskih sistemov, sporazum o vzajemnem priznavanju), dogovor o priznavanju skupnih meril (CCRA), nacionalne pobude, sektorske pobude ...	1	Ali imate vzpostavljen postopek za posodobitev ocen o kibernetski varnosti v dobavni verigi storitev in izdelkov IKT v ključnih sektorjih (kot je opredeljeno v Prilogi II direktive o varnosti omrežij in informacij (2016/1148))?	1	Ali imate sonde za odkrivanje v ključnih elementih dobavne verige, da bi odkrili zgodnje znake ogroženosti? *Npr.* varnostni nadzor na ravni ponudnikov internetnih storitev, varnostne sonde v glavnih sestavnih delih infrastrukture ...-	1

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
10 – Izboljšanje kibernetske varnosti dobavne verige	2	-		Ali v politiki javnih naročil javnih uprav uporabljate standarde za zagotovitev, da ponudniki izdelkov ali storitev IKT izpolnjujejo osnovne zahteve glede informacijske varnosti? *Npr.* ISO/IEC 27001 in 27002, ISO/IEC 27036 ...	1	Ali dejavno spodbujate najboljše prakse varnosti in vgrajene zasebnosti pri razvoju izdelkov in storitev IKT? *Npr.* varni življenjski cikel razvoja programske opreme, življenjski cikel interneta stvari	1	Ali imate vzpostavljen postopek za opredelitev šibkih členov na področju kibernetske varnosti v dobavni verigi ključnih sektorjev (kot je opredeljeno v Prilogi II direktive o varnosti omrežij in informacij (2016/1148))?	1	-	
	3	-		-		Ali razvijate in zagotavljate centralizirane kataloge z razširjenimi informacijami o obstoječih standardih za varnost informacij in zasebnosti, ki jih je mogoče nadgraditi in uporabljati za MSP?	1	Ali imate vzpostavljene mehanizme za zagotovitev, da so proizvodi in storitve IKT, ki so ključnega pomena za izvajalce bistvenih storitev, kibernetsko odporni (*tj.* sposobnost ohranjanja razpoložljivosti in varnosti pred kibernetskim incidentom) ? *Npr.* s testiranjem, rednim ocenjevanjem, odkrivanjem ogroženih elementov ...	1	-	
	4	-				Ali dejavno sodelujete pri oblikovanju certifikacijskega okvira EU za digitalne proizvode, storitve in postopke IKT, kot je določeno v aktu EU o kibernetski varnosti (Uredba (EU) 2019/881)? *Npr.* sodelovanje v Evropski certifikacijski skupini za kibernetsko varnost (ECCG), ki spodbuja tehnične standarde in postopke za varnost proizvodov/storitev IKT	0	Ali spodbujate razvoj shem certificiranja, namenjenih MSP, da bi izboljšali sprejemanje standardov za varnost informacij in zasebnost?	0	-	
	5	-		-		Ali zagotavljate kakršne koli vrste spodbud za MSP, da sprejmejo standarde varnosti in zasebnosti?	0	Ali imate vzpostavljene določbe za spodbujanje velikih podjetij, da povečajo kibernetsko varnost malih podjetij v svojih dobavnih verigah? *Npr.* vozlišče za kibernetsko varnost, usposabljanje in kampanje ozaveščanja ...	0	-	

	6	-		-		Ali spodbujate prodajalce programske opreme, da podprejo MSP z zagotavljanjem varnih privzetih konfiguracij v izdelkih, namenjenih majhnim organizacijam?	0	-		-	

4.1.3 Sklop 3: Pravo in regulativa

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
11 – Varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in ponudnikov digitalnih storitev	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali obstaja splošno razumevanje, da upravljavci kritične informacijske infrastrukture prispevajo k nacionalni varnosti?	1	Ali imate metodologijo za opredelitev bistvenih storitev?	1	Ali ste začeli izvajati direktivo o varnosti omrežij in informacij (2016/1148)?	1	Ali imate postopek za posodobitev registra tveganj?	1	Ali pripravljate in posodabljate poročila o naravi groženj?	1

	2	-		Ali imate metodologijo za opredelitev kritične informacijske infrastrukture?	1	Ali ste uvedli Direktivo o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite (št. 2008/114)?	1	Ali imate vzpostavljene druge mehanizme za merjenje, ali so tehnični in organizacijski ukrepi, ki jih izvajajo izvajalci bistvenih storitev, ustrezni za obvladovanje tveganj za varnost omrežij in informacijskih sistemov? *Npr.* redne revizije kibernetske varnosti, nacionalni okvir za izvajanje standardnih ukrepov, tehnična orodja, ki jih zagotovi vlada, kot so sonde za odkrivanje ali pregledi konfiguracij za posamezne sisteme ...	1	Ali lahko glede na najnovejši razvoj dogodkov na področju groženj v svoj akcijski načrt zaščite kritične informacijske infrastrukture vključite nov sektor?	1
	3	-		Ali imate metodologijo za opredelitev izvajalcev bistvenih storitev?	1	Ali imate nacionalni register za identificirane izvajalce bistvenih storitev po ključnih sektorjih?	1	Ali pregledujete in posodabljate seznam opredeljenih izvajalcev bistvenih storitev vsaj vsaki dve leti?	1	Ali lahko glede na najnovejši razvoj dogodkov na področju groženj svoj akcijski načrt zaščite kritične informacijske infrastrukture prilagodite novim zahtevam?	1

Cilj nacionalne strategije za kibernetsko varnost	#										
11 – Varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in ponudnikov digitalnih storitev	4	-		Ali imate metodologijo za opredelitev ponudnikov digitalnih storitev?	1	Ali imate nacionalni register za identificirane ponudnike digitalnih storitev?	1	Ali imate vzpostavljene druge mehanizme za merjenje, ali so tehnični in organizacijski ukrepi, ki jih izvajajo ponudniki digitalnih storitev, ustrezni za obvladovanje tveganj za varnost omrežij in informacijskih sistemov? *Npr.* redne revizije kibernetske varnosti, nacionalni okvir za izvajanje standardnih ukrepov, tehnična orodja, ki jih zagotovi vlada, kot so sonde za odkrivanje ali pregledi konfiguracij za posamezne sisteme ...	1	-	
	5	-		Ali imate enega ali več nacionalnih organov, ki nadzorujejo varovanje kritične informacijske infrastrukture ter varnost omrežij in informacijskih sistemov? *Npr.* v skladu z direktivo o varnosti omrežij in informacij (2016/1148)	1	Ali imate nacionalni register tveganj za ugotovljena ali znana tveganja?	1	Ali pregledujete in posodabljate seznam identificiranih ponudnikov digitalnih storitev vsaj vsaki dve leti?	1	-	
	6	-		Ali pripravljate načrte zaščite na ravni posameznih sektorjev? *Npr.* vključno z osnovnimi ukrepi za kibernetsko varnost (obvezni ukrepi ali smernice)	0	Ali imate metodologijo za kartiranje odvisnosti kritične informacijske strukture?	1	Ali uporabljate varnostno certifikacijsko shemo (nacionalno ali mednarodno) za pomoč izvajalcem bistvenih storitev in ponudnikom digitalnih storitev pri prepoznavanju varnih proizvodov IKT? *Npr.* SOG-IS MRA v Evropi, nacionalne pobude ...	1	-	
	7	-		-		Ali uporabljate prakse obvladovanja tveganja za opredelitev, količinsko opredelitev in obvladovanje tveganj, povezanih s kritično informacijsko infrastrukturo, na nacionalni ravni?	1	Ali uporabljate varnostno certifikacijsko shemo ali kvalifikacijski postopek za oceno ponudnikov storitev, ki sodelujejo z izvajalci bistvenih storitev? *Npr.* ponudniki storitev na področju odkrivanja incidentov, odzivanja na incidente, revizije kibernetske varnosti, storitev v oblaku, pametnih kartic ...	1	-	

	8	-		-		Ali sodelujete v postopku posvetovanja, da bi opredelili čezmejne odvisnosti?	1	Ali imate vzpostavljene mehanizme za merjenje ravni skladnosti izvajalcev bistvenih storitev in ponudnikov digitalnih storitev v zvezi z osnovnimi ukrepi za kibernetsko varnost?	0	-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
11 – Varovanje kritične informacijske infrastrukture, izvajalcev bistvenih storitev in ponudnikov digitalnih storitev	9					Ali imate enotno kontaktno točko, pristojno za usklajevanje vprašanj v zvezi z varnostjo omrežij in informacijskih sistemov na nacionalni ravni ter za čezmejno sodelovanje na ravni Unije?	1	Ali imate vzpostavljene določbe za zagotovitev kontinuitete storitev, ki jih zagotavljajo kritične informacijske infrastrukture? *Npr.* predvidevanje kriz, postopki za obnovo kritičnih informacijskih sistemov, neprekinjeno poslovanje brez informacijske tehnologije, postopki varnostnega kopiranja brez povezave ...	0		
	10					Ali opredeljujete osnovne ukrepe za kibernetsko varnost (obvezne ali smernice) za ponudnike digitalnih storitev in vse sektorje, opredeljene v Prilogi II k direktivi o varnosti omrežij in informacij (2016/1148)?	1				
	11	-		-		Ali zagotavljate orodja ali metodologije za odkrivanje kibernetskih incidentov?	1	-		-	

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
12 – Obravnavanje kibernetske kriminalitete	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste izvedli študijo, da bi opredelili zahteve kazenskega pregona (pravna podlaga, viri, znanja itd.) za učinkovito obravnavanje kibernetske kriminalitete?	1	Ali je vaš nacionalni pravni okvir v celoti skladen z ustreznim pravnim okvirom EU, vključno z Direktivo 2013/40/EU o napadih na informacijske sisteme? Na primer nezakonit dostop do informacijskih sistemov, nezakonito poseganje v sistem, nezakonito poseganje v podatke, nezakonito prestrezanje, orodja, ki se uporabljajo za izvedbo kaznivih dejanj ...	1	Ali imate enote, ki se ukvarjajo s kibernetsko kriminaliteto na tožilstvih?	1	Ali zbirate statistične podatke v skladu z določbami člena 14(1) Direktive 2013/40/EU (Direktiva o napadih na informacijske sisteme)?	1	Ali imate medinstitucionalno usposabljanje ali delavnice za usposabljanje organov kazenskega pregona, sodnikov, tožilcev in nacionalnih/vladnih skupin CSIRT na nacionalni in/ali večstranski ravni?	1
	2	Ali ste izvedli študijo, da bi opredelili zahteve tožilcev in sodnikov (pravna podlaga, viri, znanja itd.) za učinkovito obravnavanje kibernetske kriminalitete?	1	Ali imate kakšno pravno določbo, ki obravnava krajo identitete na spletu in krajo osebnih podatkov?	1	Ali imate posebna proračunska sredstva, dodeljena enotam za kibernetsko kriminaliteto?	1	Ali zbirate ločene statistične podatke o kibernetski kriminaliteti? *Npr.* operativne statistične podatke, statistične podatke o trendih kibernetske kriminalitete, statistične podatke o premoženjski koristi, pridobljeni s kibernetskim kriminalom, in povzročeni škodi ...	1	Ali sodelujete pri usklajenih ukrepih na mednarodni ravni za onemogočanje kriminalnih dejavnosti? *Npr.* infiltracija forumov za kriminalne vdore, organizirane skupine kibernetske kriminalitete, trgi v temnem spletu in odvzem botnetov ...	1
	3	Ali je vaša država podpisala Konvencijo Sveta Evrope o kibernetski kriminaliteti (Budimpeško konvencijo)?	1	Ali imate kakšno pravno določbo, ki obravnava kršitve pravic intelektualne lastnine in avtorskih pravic na spletu?	1	Ali ste ustanovili osrednji organ/subjekt za usklajevanje dejavnosti na področju boja proti kibernetski kriminaliteti?	1	Ali ocenjujete ustreznost usposabljanja, namenjenega organom kazenskega pregona, sodstvu in osebju nacionalnih skupin CSIRT, za obravnavanje kibernetske kriminalitete?	1	Ali obstaja jasna ločitev nalog med skupinami CSIRT, organi kazenskega pregona in sodstvom (tožilci in sodniki), kadar sodelujejo pri obravnavi kibernetske kriminalitete?	1

	4			Ali imate kakšno pravno določbo, ki obravnava nadlegovanje na spletu ali kibernetsko ustrahovanje?	1	Ali ste vzpostavili mehanizme sodelovanja med ustreznimi nacionalnimi institucijami, ki so vključene v boj proti kibernetski kriminaliteti, vključno z organi kazenskega pregona in nacionalnimi skupinami CSIRT?	1	Ali redno izvajate ocenjevanje, da bi zagotovili, da imate zadostne vire (človeške vire, proračun in orodja), namenjene enotam za kibernetsko kriminaliteto pri organih kazenskega pregona?	1	Ali vaš regulativni okvir olajšuje sodelovanje med skupinami CSIRT, organi kazenskega pregona in sodstvom (tožilci in sodniki)?	1
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**R**	
12 – Obravnavanje kibernetske kriminalitete	5			Ali imate kakšno pravno določbo, ki obravnava računalniške prevare? Npr. skladnost z določbami Konvencije Sveta Evrope o kibernetski kriminaliteti (Budimpeška konvencija).	1	Ali sodelujete in delite informacije z drugimi državami članicami na področju boja proti kibernetski kriminaliteti?	1	Ali redno izvajate ocenjevanje, da bi zagotovili, da imate zadostne vire (človeške vire, proračun in orodja), namenjene enotam za kibernetsko kriminaliteto pri organih, pristojnih za pregon?	1	Ali sodelujete pri oblikovanju in vzdrževanju standardiziranih orodij in metodologij, obrazcev in postopkov, ki jih je treba deliti z deležniki EU (organi kazenskega pregona, skupine CSIRT, agencija ENISA, Europolov EC3 ...)?	1
	6	-		Ali imate kakšno pravno določbo, ki obravnava zaščito otrok na spletu? Npr. skladnost z določbami Direktive 2011/93/EU in Budimpeške Konvencije Sveta Evrope o kibernetski kriminaliteti ...	1	Ali sodelujete in delite informacije z agencijami EU (npr. Europolov EC3, Eurojust, ENISA) na področju boja proti kibernetski kriminaliteti?	1	Ali imate enote, posebna sodišča ali specializirane sodnike za obravnavo primerov kibernetske kriminalitete?	1	Ali imate vzpostavljene napredne mehanizme, ki posameznike odvračajo od kibernetske kriminalitete ali sodelovanja v njej?	0
	7	-		Ali ste določili operativno nacionalno kontaktno točko za izmenjavo informacij in odgovarjanje na nujne zahteve drugih držav članic po informacijah v zvezi s kaznivimi dejanji iz Direktive 2013/40/EU (Direktiva o napadih na informacijske sisteme)?	1	Ali imate ustrezna orodja za obravnavo kibernetske kriminalitete? Npr. taksonomijo in klasifikacijo kibernetske kriminalitete, orodja za zbiranje elektronskih dokazov, orodja za računalniško forenziko, zaupanja vredne platforme za izmenjavo ...	1	Ali imate kakršne koli določbe, namenjene zagotavljanju podpore in pomoči žrtvam kibernetske kriminalitete (splošni uporabniki, mala in srednja podjetja, velika podjetja)?	1	Ali vaša država za učinkovito odzivanje na večje kibernetske incidente uporablja načrt EU in/ali protokol za odzivanje organov kazenskega pregona na izredne razmere (EU LE ERP)?	0
	8			Ali vaš organ kazenskega pregona vključuje posebno enoto za kibernetsko kriminaliteto?	1	Ali imate standardne operativne postopke za obravnavanje e-dokazov?	1	Ali ste vzpostavili medinstitucionalni okvir in mehanizme sodelovanja med vsemi zadevnimi deležniki (npr. organi kazenskega pregona, nacionalnimi skupinami CSIRT, pravosodnimi skupnostmi), vključno z zasebnim sektorjem (npr. izvajalci bistvenih storitev, ponudniki storitev), kadar je to primerno, da bi se odzvali na kibernetske napade?	1	-	

	9			Ali ste v skladu s členom 35 Budimpeške konvencije imenovali točko za stike, dosegljivo štiriindvajset ur na dan in sedem dni na teden?	1	Ali vaša država sodeluje pri usposabljanju, ki ga ponujajo in/ali podpirajo agencije EU (npr. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Ali vaš regulativni okvir olajšuje sodelovanje med skupinami CSIRT in organi kazenskega pregona?	1	-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
12 – Obravnavanje kibernetske kriminalitete	10	-		Ali ste imenovali operativno nacionalno točko za stike, dosegljivo štiriindvajset ur na dan in sedem dni na teden, za protokol EU za odzivanje organov kazenskega pregona na izredne razmere (EU LE ERP), da bi se odzvali na večje kibernetske napade?	1	Ali namerava vaša država sprejeti 2. dodatni protokol k Budimpeški konvenciji Sveta Evrope o kibernetski kriminaliteti?	0	Ali imate vzpostavljene mehanizme (npr. orodja, postopke) za lažjo izmenjavo informacij in sodelovanje med skupino CSIRT in organi kazenskega pregona ter po možnosti pravosodnimi organi (tožilci in sodniki) na področju boja proti kibernetski kriminaliteti?	1	-	
	11			Ali redno zagotavljate specializirano usposabljanje za deležnike, ki se ukvarjajo s kibernetsko kriminaliteto (organi kazenskega pregona, sodstvo, skupine CSIRT)? Npr. usposabljanja o prijavljanju/pregonu kriminalitete, ki jo omogoča kibernetski prostor, usposabljanja o zbiranju elektronskih dokazov in zagotavljanju integritete v digitalni nadzorni verigi in računalniški forenziki.	1						
	12			Ali je vaša država ratificirala Konvencijo Sveta Evrope o kibernetski kriminaliteti (Budimpeško konvencijo) oz. k njej pristopila?	1			-	-	-	
	13	-		Ali je vaša država podpisala in ratificirala Dodatni protokol (inkriminacija rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih) h Konvenciji Sveta Evrope o kibernetski kriminaliteti (Budimpeški konvenciji)?	0	-	-	-		-	

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
13 – Vzpostavitev mehanizmov za poročanje o incidentih	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali imate med zasebnimi organizacijami in nacionalnimi organi vzpostavljene neformalne mehanizme za izmenjavo informacij o incidentih na področju kibernetske varnosti?	1	Ali imate sistem poročanja o incidentih za vse sektorje iz Priloge II k direktivi o varnosti omrežij in informacij?	1	Ali imate sistem obveznega poročanja o incidentih, ki deluje v praksi?	1	Ali imate usklajen postopek za sektorske sisteme poročanja o incidentih?	1	Ali ustvarite letno poročilo o incidentih?	1
	2	-		Ali ste v skladu s členom 40 Direktive (EU 2018/1972) uvedli zahteve glede priglasitve za ponudnike telekomunikacijskih storitev? Direktiva zahteva, da države članice zagotovijo, da ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev brez nepotrebnega odlašanja uradno obvestijo pristojni organ o kibernetskem incidentu, ki je znatno vplival na delovanje omrežij ali storitev.	1	Ali obstaja mehanizem usklajevanja/sodelovanja za obveznosti poročanja o incidentih v zvezi s Splošno uredbo o varstvu podatkov, direktivo o varnosti omrežij in informacij, členom 40 (prejšnji člen 13a) in Uredbe eIDAS?	1	Ali imate sistem poročanja o incidentih za sektorje, ki niso zajeti v direktivi o varnosti omrežij in informacij?	1	Ali obstajajo kakšna poročila s področja kibernetske varnosti ali druge vrste analiz, ki jih pripravi subjekt, ki prejme poročila o incidentih?	1

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
13 – Vzpostavitev mehanizmov za poročanje o incidentih	3	-		Ali ste uvedli zahteve glede obveščanja za ponudnike storitev zaupanja v skladu s členom 19 Uredbe eIDAS (Uredba (EU) št. 910/2014)? Člen 19 med drugim zahteva, da ponudniki storitev zaupanja obvestijo nadzorni organ o pomembnih incidentih/kršitvah varnosti.	1	Ali imate ustrezna orodja za zagotavljanje zaupnosti in celovitosti informacij, ki se izmenjujejo prek različnih kanalov za prijavo?	1	Ali merite učinkovitost postopkov za poročanje o incidentih? *Npr.* kazalniki o incidentih, ki so bili sporočeni po ustreznih kanalih, časovni okvir poročila o incidentu ...	1	-	
	4	-		Ali ste v skladu s členom 16 direktive o varnosti omrežij in informacij uvedli zahteve glede priglasitve za ponudnike digitalnih storitev? Člen 16 zahteva, da ponudniki digitalnih storitev vsak incident, ki ima pomemben vpliv na zagotavljanje storitve iz Priloge III, ki jo ponujajo v Uniji, brez nepotrebnega odlašanja priglasijo pristojnemu organu ali skupini CSIRT.	1	Ali imate platformo/orodje za olajšanje postopka poročanja?	0	Ali imate na nacionalni ravni skupno taksonomijo za razvrščanje incidentov in kategorije temeljnih vzrokov?	0	-	

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
14 – Okrepitev zasebnosti in varstva podatkov	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali ste izvedli študije ali analize za opredelitev področij, na katerih so potrebne izboljšave, za boljšo zaščito pravic do zasebnosti državljanov?	1	Ali je nacionalni organ za varstvo podatkov vključen v vprašanja, povezana s kibernetsko varnostjo (npr. priprava novih zakonov in predpisov o kibernetski varnosti, opredeljeni minimalni varnostni ukrepi)?	1	Ali spodbujate najboljše prakse v zvezi z varnostnimi ukrepi in vgrajenim varstvom podatkov za javni in/ali zasebni sektor?	1	Ali redno izvajate ocenjevanje, da bi zagotovili, da imate zadostne vire (človeške vire, proračun in orodja), namenjene organu za varstvo podatkov?	1	Ali imate vzpostavljene mehanizme za spremljanje najnovejšega tehnološkega razvoja, da bi prilagodili ustrezne smernice in pravne določbe/obveznosti?	1
	2	Ali ste na nacionalni ravni razvili pravno podlago za izvajanje Splošne uredbe o varstvu podatkov (Uredba (EU) št. 2016/679)? Npr. ohranili ali uvedli bolj specifične določbe ali omejitve pravil Uredbe	0	-		Ali uvajate programe ozaveščanja in usposabljanja o tej temi?	1	Ali spodbujate organizacije in podjetja, da pridobijo certifikat ISO/IEC 27701:2019 o sistemu upravljanja osebnih podatkov (PIMS)?	1	Ali dejavno sodelujete/spodbujate pobude na področju raziskav in razvoja v zvezi s tehnologijami za boljše varovanje zasebnosti (PET)?	0
	3	-		-		Ali postopke poročanja o incidentih usklajujete z organom za varstvo podatkov?	1	-		-	
	4	-		-		Ali spodbujate in podpirate razvoj tehničnih standardov o varnosti informacij in zasebnosti? Ali so posebej prilagojeni malim in srednjim podjetjem (MSP)?	0	-		-	
	5	-		-		Ali zagotavljate praktične in nadgradljive smernice za podporo različnim vrstam upravljavcev podatkov pri izpolnjevanju pravnih zahtev in obveznosti glede zasebnosti in varstva podatkov?	0	-		-	

4.1.4 Sklop 4: Sodelovanje

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
15 – Vzpostavitev javno-zasebnega partnerstva (JZP)	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali se na splošno razume, da javno-zasebna partnerstva prispevajo k zvišanju ravni kibernetske varnosti v državi na različne načine? *Npr.* z delitvijo interesov za rast industrije kibernetske varnosti, sodelovanjem pri oblikovanju ustreznega regulativnega okvira za kibernetsko varnost, spodbujanjem raziskav in razvoja ...	1	Ali imate nacionalni akcijski načrt za ustanovitev javno-zasebnih partnerstev?	1	Ali ste ustanovili nacionalna javno-zasebna partnerstva?	1	Ali ste ustanovili medsektorska javno-zasebna partnerstva?	1	Ali lahko glede na najnovejši tehnološki in regulativni razvoj prilagodite ali ustvarite javno-zasebna partnerstva?	1
	2	-		Ali vzpostavite pravno ali pogodbeno podlago (posebni zakoni, sporazumi o nerazkritju informacij, intelektualna lastnina) za določitev področja uporabe javno-zasebnih partnerstev?	1	Ali ste vzpostavili sektorska javno-zasebna partnerstva?	1	Ali se v vzpostavljenih javno-zasebnih partnerstvih osredotočate tudi na javno-javno in zasebno-zasebno sodelovanje?	1		
	3	-		-		Ali zagotavljate finančna sredstva za vzpostavitev javno-zasebnih partnerstev?	1	Ali spodbujate javno-zasebna partnerstva med malimi in srednjimi podjetji (MSP)?	1	-	

	4	-		-		Ali javne institucije na splošno vodijo javno-zasebna partnerstva? *Tj.* enotna točka stika iz javnega sektorja, ki upravlja in usklajuje javno-zasebno partnerstvo, javni organi se vnaprej dogovorijo o tem, kaj želijo doseči, jasne smernice javnih uprav o njihovih potrebah in omejitvah v zasebnem sektorju ...	1	Ali merite rezultate javno-zasebnih partnerstev?	1	-	
	5	-		-		Ali ste član pogodbenega javno-zasebnega partnerstva Evropske organizacije za kibernetsko varnost (ECSO)?	0	-		-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
15 – Vzpostavitev javno-zasebnega partnerstva (JZP)	6	-		-		Ali imate eno ali več javno-zasebnih partnerstev, ki se ukvarjajo z dejavnostmi skupine CSIRT?	0	-		-	
	7					Ali imate eno ali več javno-zasebnih partnerstev, ki se ukvarjajo z vprašanji zaščite kritične informacijske infrastrukture?	0				
	8	-		-		Ali imate eno ali več javno-zasebnih partnerstev, ki se ukvarjajo z ozaveščanjem in razvojem znanj in spretnosti na področju kibernetske varnosti?	0	-		-	

Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
16 – Institucionalizacija sodelovanja med javnimi agencijami	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1

	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali imate vzpostavljene kanale neformalnega sodelovanja med javnimi agencijami?	1	Ali imate nacionalni program sodelovanja, ki se osredotoča na kibernetsko varnost? *Npr.* svetovalni odbori, usmerjevalne skupine, forumi, sveti, kibernetska središča ali skupine za srečanja strokovnjakov.	1	Ali javni organi sodelujejo v programu sodelovanja?	1	Ali zagotavljate, da obstajajo kanali za sodelovanje, namenjeni kibernetski varnosti, vsaj med naslednjimi javnimi organi: obveščevalne službe, nacionalni organi kazenskega pregona, organi pregona, vladni akterji, nacionalna skupina CSIRT in vojska?	1	Ali imajo javne agencije na voljo enotne minimalne informacije o najnovejšem razvoju dogodkov na področju groženj in ozaveščenosti o razmerah na področju kibernetske varnosti?	1
	2	-		-		Ali ste vzpostavili platforme za sodelovanje za izmenjavo informacij?	1	Ali merite uspehe in omejitve različnih programov sodelovanja pri spodbujanju učinkovitega sodelovanja?	1	-	
Cilj nacionalne strategije za kibernetsko varnost	**#**	**Raven 1:**	**P**	**Raven 2:**	**P**	**Raven 3**	**P**	**Raven 4**	**P**	**Raven 5**	**P**
16 – Institucionalizacija sodelovanja med javnimi agencijami	3	-		-		Ali ste opredelili obseg platform za sodelovanje (npr. naloge in odgovornosti, število tematskih področij)?	1	-		-	
	4	-		-		Ali organizirate letna srečanja?	1	-		-	
	5	-		-		Ali imate vzpostavljene mehanizme sodelovanja med pristojnimi organi po geografskih regijah? *Npr.* mreža korespondentov za varnost po regijah, uradnik za kibernetsko varnost v regionalnih gospodarskih zbornicah ...	1	-		-	

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
17 – Mednarodno sodelovanje (ne samo z državami članicami EU)	p	Ali je cilj zajet v vaši trenutni nacionalni strategiji za kibernetsko varnost oz. ali ga nameravate zajeti v naslednji izdaji le-te?	1	Ali obstajajo neformalne prakse ali aktivnosti, ki prispevajo k doseganju cilja na neusklajen način?	1	Ali imate akcijski načrt, ki je formalno opredeljen in dokumentiran?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da bi preverili njegovo izvajanje/uspešnost?	1	Ali imate vzpostavljene mehanizme, ki zagotavljajo, da je akcijski načrt dinamično prilagojen dogodkom/spremembam v okolju?	1
	b			Ali ste opredelili načrtovane rezultate, vodilna načela ali ključne aktivnosti svojega akcijskega načrta?	1	Ali imate akcijski načrt z jasno začrtanim načinom dodeljevanja sredstev in upravljanjem?	1	Ali pregledujete svoj akcijski načrt z vidika cilja, da se zagotovi pravilna opredelitev prednostnih nalog in njegova optimizacija?	1		
	c			Če je ustrezno, ali se vaš akcijski načrt izvaja in je v omejenem obsegu že učinkovit?	0						
	1	Ali imate strategijo mednarodnega delovanja?	1	Ali imate sporazume o sodelovanju z drugimi državami (dvostranski, večstranski sporazumi) ali partnerji v drugih državah? *Npr.* na področju izmenjave informacij, krepitve zmogljivosti, pomoči ...	1	Ali izmenjujete informacije na strateški ravni? *Npr.* politika na visoki ravni, zaznavanje tveganja ...	1	Ali so nacionalne javne agencije za kibernetsko varnost v vaši državi vključene v programe mednarodnega sodelovanja?	1	Ali vodite razprave o eni ali več temah v okviru večstranskih sporazumov?	1
	2	Ali imate vzpostavljene neformalne kanale za sodelovanje z drugimi državami?	1	Ali imate enotno kontaktno točko, ki lahko opravlja povezovalno funkcijo za zagotavljanje čezmejnega sodelovanja z organi držav članic (skupina za sodelovanje, mreža skupin CSIRT ...)?	1	Ali si izmenjujete informacije na taktični ravni? *Npr.* bilten o akterjih groženj, center za izmenjavo in analizo informacij (ISAC), TTP ...	1	Ali redno ocenjujete rezultate pobud za mednarodno sodelovanje?	1	Ali vodite razprave o eni ali več temah v okviru mednarodnih pogodb ali konvencij?	1

Cilj nacionalne strategije za kibernetsko varnost	#	Raven 1:	P	Raven 2:	P	Raven 3	P	Raven 4	P	Raven 5	P
17 – Mednarodno sodelovanje (ne samo z državami članicami EU)	3	Ali je javni sektor izrazil namero, da se vključi v mednarodno sodelovanje na področju kibernetske varnosti?	1	Ali imate ljudi, ki se ukvarjajo z vključevanjem v mednarodno sodelovanje?	1	Ali izmenjujete informacije na operativni ravni? *Npr.* informacije o operativnem usklajevanju, tekoči incidenti, začetne operativne zmogljivosti ...	1	-		Ali vodite razprave ali pogajanja o eni ali več temah v okviru mednarodnih skupin strokovnjakov? *Npr.* svetovna komisija za stabilnost v kibernetskem prostoru (GCSC), skupina agencije ENISA za sodelovanje na področju varnosti omrežij in informacij, skupina vladnih strokovnjakov ZN za informacijsko varnost (GGE) ...	1
	4	-		-		Ali sodelujete v mednarodnih vajah na področju kibernetske varnosti?	1	-		-	

	5	-		-		Ali sodelujete v mednarodnih pobudah za krepitev zmogljivosti? *Npr.* usposabljanja , razvoj znanj in spretnosti, priprava standardnih postopkov ...	0	-		-	
	6	-		-		Ali ste sklenili sporazume o medsebojni pomoči z drugimi državami? *Npr.* dejavnosti organov kazenskega pregona, sodni postopki, združitev zmogljivosti odzivanja na incidente, skupna uporaba sredstev za kibernetsko varnost ...	0	-		-	
	7	-		-		Ali ste podpisali ali ratificirali mednarodne pogodbe ali konvencije na področju kibernetske varnosti? *Npr.* mednarodni kodeks ravnanja za varnost informacij, Konvencija o kibernetski kriminaliteti	0	-		-	

4.2 SMERNICE ZA UPORABO OKVIRJA

Namen tega poglavja je državam članicam zagotoviti nekaj smernic in priporočil za uvajanje okvirja in izpolnjevanje vprašalnika. Spodaj navedena priporočila izhajajo predvsem iz povratnih informacij, zbranih na razgovorih s predstavniki držav članic:

- **Predvidite usklajevalne dejavnosti za zbiranje podatkov in konsolidacijo podatkov.** Večina držav članic ugotavlja, da bi morala izvedba takega samoocenjevanja trajati približno 15 delovnih dni na osebo. Za izvedbo samoocenjevanja bo treba pritegniti veliko različnih deležnikov. Zato se priporoča, da se v okviru pripravljalne faze določi čas za opredelitev vseh ustreznih deležnikov v vladnih organih, javnih agencijah in zasebnem sektorju.
- **Opredelite osrednji organ, ki bo odgovoren za dokončanje samoocenjevanja na nacionalni ravni.** Ker lahko zbiranje gradiva za vse kazalnike okvira NCAF vključuje številne deležnike, se priporoča, da opredelite osrednji organ ali agencijo, ki bo imela nalogo, da dokonča samoocenjevanje, tako da povezuje in usklajuje vse zadevne deležnike.
- **Ocenjevanje uporabite kot način za izmenjavo in komuniciranje o temah v zvezi s kibernetsko varnostjo.** Pridobljene izkušnje, ki so jih izmenjale države članice, so pokazale, da so razprave (bodisi v obliki individualnih razgovorov ali skupinskih delavnic) dobra priložnost za spodbujanje dialoga o temah kibernetske varnosti ter za izmenjavo skupnih stališč in področij, na katerih so potrebne izboljšave. Izmenjava rezultatov lahko poleg osvetlitve ključnih dosežkov prispeva tudi k promociji tem s področja kibernetske varnosti.
- **Uporabite nacionalno strategijo za kibernetsko varnost kot okvir za izbiro ciljev, na katere se nanaša ocena.** Sedemnajst (17) ciljev, ki sestavljajo okvir NCAF, je bilo oblikovanih na podlagi ciljev, ki jih države članice običajno zajemajo v svojih nacionalnih strategijah za kibernetsko varnost. Cilje, zajete kot del nacionalne strategije za kibernetsko varnost, bi bilo treba uporabiti kot sredstvo za postavitev obsega ocene. Vendar nacionalna strategija za kibernetsko varnost ne bi smela omejevati ocene. Ker se nacionalna strategija za kibernetsko varnost osredotoča na prednostne naloge, so nekatera področja namenoma izpuščena iz nje. Vendar to ne pomeni, da določena zmogljivost ni prisotna. Na primer, kadar nacionalna strategija za kibernetsko varnost ne vsebuje določenega cilja, vendar pa ima država zmogljivosti na področju kibernetske varnosti, ki so povezane s tem ciljem, se lahko ta cilj oceni.
- **Ko se področje uporabe nacionalne strategije za kibernetsko varnost razvija, zagotovite, da bo razlaga ocene še naprej skladna z razvojem nacionalne strategije za kibernetsko varnost.** Življenjski cikel nacionalne strategije za kibernetsko varnosti je večletni proces. Nacionalna strategija za kibernetsko varnost nekaterih držav članic se običajno izvaja v okviru 3- do 5-letnega načrta, pri čemer prihaja do sprememb obsega med dvema zaporednima izdajama nacionalne strategije za kibernetsko varnost. V zvezi s tem je treba posebno pozornost nameniti predstavitvi rezultatov samoocenjevanja med dvema izdajama nacionalne strategije za kibernetsko varnost: spremembe v obsegu lahko vplivajo na končno oceno zrelosti. Priporoča se, da se primerjajo ocene celotnega obsega strateških ciljev enega leta z ocenami drugega leta (*tj.* skupna splošna ocena).

Opomnik o mehanizmu točkovanja – primer deleža pokritosti
Mehanizem točkovanja vključuje dve ravni ocen:
(i) **skupni splošni delež pokritosti,** ki temelji na celotnem seznamu strateških ciljev iz okvira za samoocenjevanje;
(ii) **skupni specifični delež pokritosti**, ki temelji na strateških ciljih, ki jih izbere država članica (običajno ustreza ciljem iz nacionalne strategije za kibernetsko varnost posamezne države).

Po zasnovi (glej poglavje 3.1 o mehanizmu točkovanja) bo skupni specifični delež pokritosti enak skupnemu splošnemu deležu pokritosti ali višji od njega, saj lahko slednji vključuje cilje, ki

jih država članica ne pokriva. Zaradi tega se skupni splošni delež pokritosti zniža. Če država članica doda nov cilj, se bo skupni delež pokritosti povečal (tj. zajetih je več kazalnikov zrelosti), medtem ko se lahko skupna specifična zrelost zmanjša (če je novo dodani cilj v začetni fazi in ima zato nizko stopnjo zrelosti).

- **Pri izpolnjevanju vprašalnika za samoocenjevanje upoštevajte, da je njegov glavni cilj podpora državam članicam pri krepitvi zmogljivosti na področju kibernetske varnosti.** Zato je pri izpolnjevanju vprašalnika priporočljivo izbrati odgovor, ki je najbolj splošno sprejet, čeprav je v nekaterih primerih težko podati jasen odgovor. Če je na primer odgovor na vprašanje pritrdilen (DA) glede na določeno področje, vendar je na drugem področju odgovor NE, bi morale države članice upoštevati, da odgovor NE zahteva ukrepanje: bodisi načrt izboljšanja bodisi načrt za ukrepanje na področju izboljšav, ki ga je treba upoštevati pri prihodnjem razvoju.

5. NASLEDNJI KORAKI

5.1 IZBOLJŠAVE V PRIHODNOSTI

Med razgovori s predstavniki držav članic in med fazo teoretičnega raziskovanja so bila kot možni prihodnji razvoj opredeljena tudi naslednja priporočila za izboljšanje sedanjega okvira za ocenjevanje nacionalnih zmogljivosti:

- **Razvoj sistema točkovanja, da se omogoči večja natančnost.** Namesto binarnih odgovorov DA/NE bi lahko na primer uvedli odstotek pokritosti, da bi bolje upoštevali zapletenost konsolidacije zmogljivosti na nacionalni ravni. Kot prvi korak je bil izbran preprost pristop z odgovori DA/NE.
- **Uvedba kvantitativnih metrik za merjenje učinkovitosti nacionalnih strategij za kibernetsko varnost posameznih držav članic.** Okvir za ocenjevanje nacionalnih zmogljivosti se osredotoča na ocenjevanje ravni zrelosti zmogljivosti držav članic na področju kibernetske varnosti. To bi lahko dopolnili z metriko za merjenje učinkovitosti dejavnosti in akcijskih načrtov, ki jih izvajajo države članice za izgradnjo teh zmogljivosti. Oblikovanje takih meril uspešnosti se v sedanji fazi ni zdelo realistično, saj obstaja malo povratnih informacij s tega področja, obstajajo pa tudi težave pri iskanju smiselnih kazalnikov, ki povezujejo učinke z izvajanjem nacionalne strategije za kibernetsko varnost, in težave pri oblikovanju realističnih kazalnikov, ki jih je mogoče naknadno zbrati. Vsekakor to ostaja tema, ki jo je treba nasloviti v prihodnosti.
- **Prehod od samoocenjevanja na ocenjevanje.** Možen razvoj okvira v prihodnosti bi lahko bila preusmeritev k ocenjevanju, da bi se zrelost zmogljivosti držav članic na področju kibernetske varnosti bolj dosledno ocenjevala. Če bi oceno izvedla tretja oseba, bi se lahko zmanjšala morebitna pristranskost.

PRILOGA A – PREGLED REZULTATOV TEORETIČNE RAZISKAVE

Priloga A vsebuje povzetek predhodnega dela agencije ENISA v zvezi z nacionalno strategijo za kibernetsko varnost in pregled ustreznih javno dostopnih zrelostnih modelov na področju zmogljivosti kibernetske varnosti. Pri izbiri in pregledu modelov se upoštevajo naslednje predpostavke:

- vsi modeli ne temeljijo na strogi raziskovalni metodologiji;
- struktura in rezultati modelov niso vedno podrobno pojasnjeni z jasnimi povezavami med različnimi elementi, ki so značilni za posamezni model;
- nekateri modeli ne ponujajo podrobnosti o razvojnem procesu, strukturi in metodologiji ocenjevanja;
- drugi modeli in orodja, ki smo jih odkrili, ne vsebujejo podrobnosti o strukturi in vsebini, zato niso navedeni;
- izbira modelov za pregled temelji na geografski pokritosti. Glavni poudarek bo na zrelostnih modelih na področju zmogljivosti kibernetske varnosti, ki so bili zasnovani za oceno uspešnosti evropskih držav. Vendar je pomembno razširiti geografsko pokritost, da se analizirajo dobre prakse pri oblikovanju modelov zrelosti po vsem svetu.

Ta sistematični pregled ustreznih javno dostopnih zrelostnih modelov na področju zmogljivosti kibernetske varnosti je bil izveden z uporabo prilagojenega okvira analize, ki temelji na metodologiji, ki jo je za razvoj zrelostnih modelov opredelil Becker[22]. Za vsak obstoječi zrelostni model so bili analizirani naslednji elementi:

- **ime zrelostnega modela:** ime zrelostnega modela in glavne reference;
- **institucija:** javna ali zasebna institucija, ki je odgovorna za oblikovanje modela;
- **splošni namen in cilj:** splošno področje uporabe modela in predvideni cilji;
- **število in opredelitev ravni:** število ravni zrelosti modela in njihov splošni opis;
- **število in ime značilnosti/atributov:** število in ime atributov, ki jih uporablja zrelostni model. Analiza atributov ima trojni cilj:
  - razčleniti zrelostni model v enostavno razumljive razdelke;
  - združi več atributov v sklope atributov, ki izpolnjujejo isti cilj;
  - navesti različna stališča glede predmeta ravni zrelosti.
- **metoda ocenjevanja:** metoda ocenjevanja zrelostnega modela;

[22] J. Becker, R. Knackstedt in J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application" *(Razvoj zrelostnih modelov za upravljanje IT: Model postopka in njegova uporaba)*, Business & Information Systems Engineering, let. 1, št. 3, str. 213–222, Junij 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

- **prikaz rezultatov**: opredeliti metodo vizualizacije rezultatov zrelostnega modela. Logika tega koraka je, da so modeli zrelosti običajno neuspešni, če so preveč zapleteni, zato mora način prikaza zadovoljevati praktične potrebe.

Predhodno delo v zvezi z nacionalno strategijo za kibernetsko varnost

Agencija ENISA je leta 2012 v okviru svojih zgodnjih prizadevanj objavila dva dokumenta na temo nacionalnih strategij za kibernetsko varnost. Najprej je bil v „Praktičnem vodniku za razvojno in izvedbeno fazo nacionalne strategije za kibernetsko varnost“[23] predlagan sklop konkretnih ukrepov za učinkovito izvajanje nacionalne strategije za kibernetsko varnost in predstavljen življenjski cikel nacionalne strategije za kibernetsko varnost v štirih fazah: razvoj strategije, izvajanje strategije, vrednotenje strategije in vzdrževanje strategije. V drugem dokumentu z naslovom „Določitev poti za nacionalna prizadevanja za okrepitev varnosti v kibernetskem prostoru“[24] (objavljenem leta 212) je bil opisan status strategij za kibernetsko varnost v EU in zunaj nje ter predlagano, naj države članice določijo skupne teme in razlike med svojimi nacionalnimi strategijami za kibernetsko varnost.

Leta 2014 je bil objavljen prvi okvir agencije ENISA za ocenjevanje nacionalnih strategij za kibernetsko varnost držav članic[25]. Ta okvir vsebuje priporočila in dobre prakse ter sklop orodij za krepitev zmogljivosti za ocenjevanje nacionalne strategije za kibernetsko varnost (*npr.* opredeljeni cilji, vložki, učinki, ključni kazalniki uspešnosti ...). Ta orodja so prilagojena različnim potrebam držav z različno ravnjo zrelosti pri njihovem strateškem načrtovanju. Istega leta je agencija ENISA objavila „Spletni interaktivni zemljevid nacionalnih strategij za kibernetsko varnost“[26], ki uporabnikom omogoča, da se hitro seznanijo z nacionalnimi strategijami za kibernetsko varnost vseh držav članic in držav EFTA, vključno z njihovimi strateškimi cilji in dobrimi primeri izvajanja. Najprej je bil razvit kot Zbirka (repozitorij) nacionalnih strategij za kibernetsko varnost (2014), nato je bil leta 2018 posodobljen s primeri izvajanja, od leta 2019 pa zemljevid deluje kot *informacijsko vozlišče* za centralizacijo podatkov, ki jih zagotavljajo države članice, o njihovih prizadevanjih za izboljšanje nacionalne kibernetske varnosti.

„Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost“[27], ki je bil objavljen leta 2016, opredeljuje petnajst strateških ciljev. V tem vodniku je analizirano stanje izvajanja nacionalne strategije za kibernetsko varnost vsake države članice, opredeljene pa so tudi različne vrzeli in izzivi v zvezi s tem izvajanjem.

[23] NCSS: Practical Guide on Development and Execution (Nacionalna strategija za kibernetsko varnost: Praktični vodnik o razvoju in izvajanju) (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Nacionalna strategija za kibernetsko varnost: Določitev poti za nacionalna prizadevanja za okrepitev varnosti v kibernetskem prostoru) (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (Okvir ocenjevanja za nacionalne strategije kibernetske varnosti) (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (Nacionalne strategije za kibernetsko varnost – interaktivni zemljevid) (ENISA, 2014, posodobljeno 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Ta dokument posodablja vodnik iz leta 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost: oblikovanje in izvajanje nacionalnih strategij za kibernetsko varnost) (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
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

Agencija ENISA je nato leta 2018 objavila „Orodje za ocenjevanje nacionalnih strategij za kibernetsko varnost“[28]: interaktivno orodje za samoocenjevanje, ki državam članicam pomaga pri vrednotenju njihovih strateških prednostnih nalog in ciljev, povezanih z njihovo nacionalno strategijo za kibernetsko varnost. S sklopom preprostih vprašanj to orodje državam članicam zagotavlja posebna priporočila za izvajanje posameznih ciljev. Nazadnje so v dokumentu „Dobre prakse pri inovacijah na področju kibernetske varnosti v okviru nacionalne strategije za kibernetsko varnost“[29], objavljenem leta 2019, predstavljene inovacije na področju kibernetske varnosti v okviru nacionalne strategije za kibernetsko varnost. V dokumentu so predstavljeni izzivi in dobre prakse v različnih razsežnostih inovacij, kot jih dojemajo strokovnjaki s področja, da bi bili v pomoč pri oblikovanju prihodnjih inovativnih strateških ciljev.

A.1 Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM)

Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM) je razvil Svetovni center za zmogljivosti na področju kibernetske varnosti (Center za zmogljivost – Capacity Centre), ki je del šole Oxford Martin School na Univerzi v Oxfordu. Cilj Centra za zmogljivost je povečati obseg in učinkovitost krepitve zmogljivosti na področju kibernetske varnosti v Združenem kraljestvu in na mednarodni ravni z uvedbo zrelostnega modela za zmogljivosti na področju kibernetske varnosti (model CMM). Model CMM je neposredno usmerjen v države, ki želijo povečati svoje nacionalne zmogljivosti na področju kibernetske varnosti. Prvotno je bil uveden leta 2014, leta 2016 pa je bil revidiran, potem ko je bil uporabljen pri pregledu 11 nacionalnih zmogljivosti na področju kibernetske varnosti.

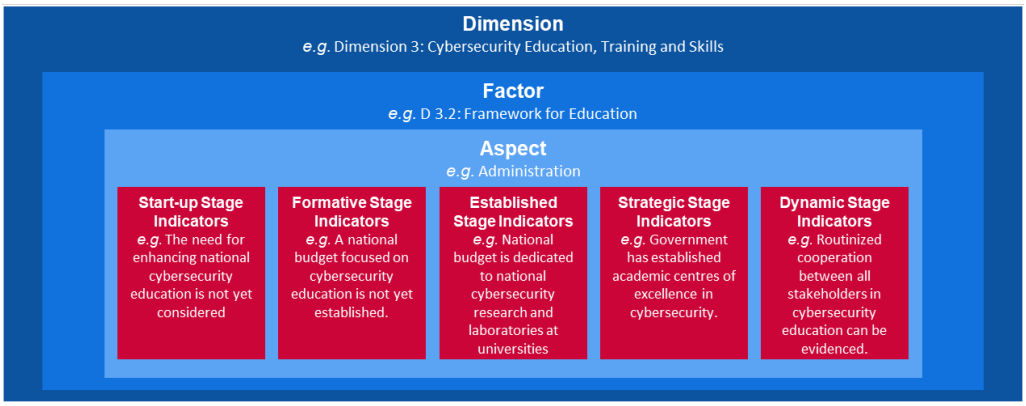
Atributi/razsežnosti

Model CMM predpostavlja, da zmogljivost na področju kibernetske varnosti obsega **pet razsežnosti**, ki predstavljajo sklope zmogljivosti kibernetske varnosti. Vsak sklop predstavlja drugačno raziskovalno „lečo“, skozi katero je mogoče preučiti in razumeti zmogljivosti na področju kibernetske varnosti. V okviru petih razsežnosti so predstavljeni **dejavniki**, ki opisujejo podrobnosti o zmogljivosti na področju kibernetske varnosti. Te podrobnosti so elementi, ki prispevajo k izboljšanju zrelosti zmogljivosti na področju kibernetske varnosti v okviru posamezne razsežnosti. Za vsak dejavnik je več **vidikov**, ki predstavljajo različne sestavine dejavnika. Vidiki predstavljajo organizacijsko metodo za razdelitev kazalnikov na manjše skupine, ki jih je lažje razumeti. Vsak vidik se nato oceni s **kazalniki**, ki opisujejo korake, ukrepe ali gradnike, ki kažejo na določeno stopnjo zrelosti (opredeljeno v naslednjem poglavju) v okviru posebnega vidika, dejavnika in razsežnosti.

Zgoraj navedeni izrazi so lahko večplastni, kot je prikazano na spodnji sliki.

[28] National Cybersecurity Strategies Evaluation Tool (Orodje za ocenjevanje nacionalnih strategij za kibernetsko varnost) (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

Slika 4: Primer kazalnikov modela CMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Razsežnost npr. razsežnost 3: izobraževanje, usposabljanje in spretnosti na področju kibernetske varnosti
Factor e.g. D 3.2: Framework for Education	Dejavnik npr. D 3.2: okvir za izobraževanje
Aspect e.g. Administration	Vidik npr. uprava
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Kazalniki faze zagona npr. o potrebi za izboljšanje nacionalnega izobraževanja o kibernetski varnosti se še ne razmišlja
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Kazalniki faze oblikovanja npr. nacionalni proračun, osredotočen na izobraževanje o kibernetski varnosti, še ni določen
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Kazalniki faze vzpostavitve npr. nacionalni proračun je namenjen nacionalnim raziskavam in laboratorijem na področju kibernetske varnosti na univerzah
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Kazalniki strateške faze npr. vlada je ustanovila akademski center odličnosti na področju kibernetske varnosti
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Kazalniki dinamične faze npr. dokazati je mogoče rutinsko sodelovanje med vsemi deležniki pri izobraževanju o kibernetski varnosti

Spodaj je podrobno opisanih pet razsežnosti:

i oblikovanje politike in strategije za kibernetsko varnost (6 dejavnikov);
ii spodbujanje odgovorne kulture na področju kibernetske varnosti v družbi (5 dejavnikov);
iii razvoj znanja o kibernetski varnosti (3 dejavniki);
iv oblikovanje učinkovitih pravnih in regulativnih okvirov (3 dejavniki);
v nadzor tveganj s pomočjo standardov, organizacij in tehnologij (7 dejavnikov).

Ravni zrelosti

Model CMM uporablja **5 ravni zrelosti** za določitev, v kolikšni meri je država napredovala v zvezi z določenim dejavnikom/vidikom zmogljivosti na področju kibernetske varnosti. Te ravni služijo kot pregled obstoječih zmogljivosti na področju kibernetske varnosti:

- **faza zagona:** na tej stopnji zrelost na področju kibernetske varnosti ne obstaja ali pa je še v nerazviti fazi. Morda potekajo začetne razprave o krepitvi zmogljivosti na področju kibernetske varnosti, vendar konkretni ukrepi niso bili sprejeti. Na tej stopnji ni dokazov, ki bi jih bilo mogoče opazovati;

- **faza oblikovanja:** nekateri vidiki so se začeli širiti in oblikovati, vendar so lahko ad hoc narave, neorganizirani, slabo opredeljeni – ali preprosto „novi“. Vendar je mogoče dokaze o tej dejavnosti jasno prikazati;
- **faza vzpostavitve:** elementi tega vidika so vzpostavljeni in delujejo. Vendar pa s tem povezana razporeditev sredstev ni dobro premišljena. V zvezi s „povezanimi“ naložbami v različne elemente tega vidika je bilo sprejetih malo kompromisov pri sprejemanju določitev. Vendar je ta vidik funkcionalen in opredeljen;
- **strateška faza:** sprejete so bile odločitve o tem, kateri deli tega vidika so pomembni in kateri so manj pomembni za posamezno organizacijo ali državo. Strateška faza odraža dejstvo, da so bile te odločitve sprejete glede na posebne okoliščine države ali organizacije;
- **dinamična faza**: v tej fazi so vzpostavljeni jasni mehanizmi za spreminjanje strategije glede na prevladujoče okoliščine, kot so tehnologija v okolju groženj, svetovni konflikti ali pomembne spremembe na enem zadevnem področju (*npr.* kibernetska kriminaliteta ali zasebnost). Dinamične organizacije so razvile metode za sprotno spreminjanje strategij. Na tej stopnji so značilni hitro odločanje, prerazporejanje virov in stalna pozornost na spreminjajoče se razmere.

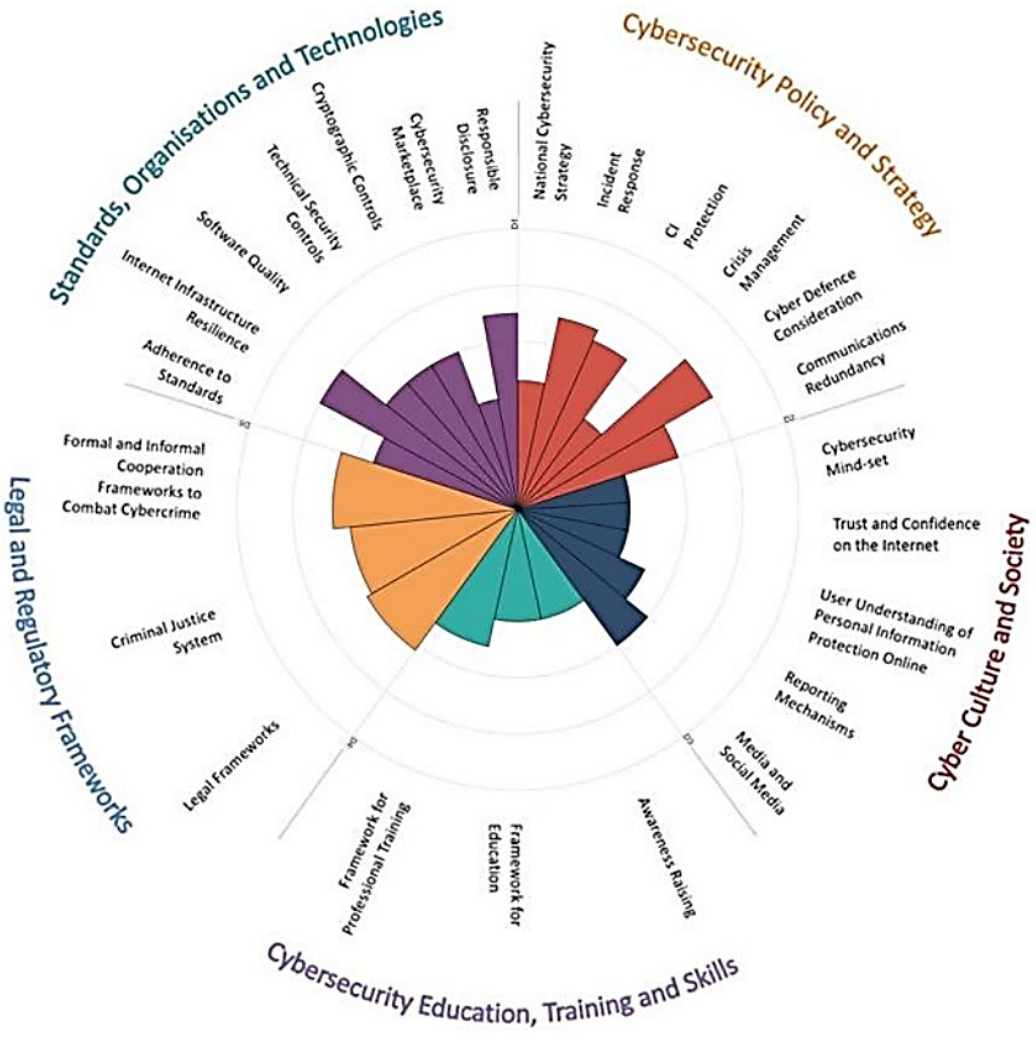
Metoda ocenjevanja

Ker Center za zmogljivost nima poglobljenega razumevanja posameznega nacionalnega okvira, v katerem se model uvaja, sodeluje z mednarodnimi organizacijami, ministrstvi ali organizacijami gostiteljicami v zadevni državi pri pregledu zrelosti zmogljivosti na področju kibernetske varnosti. Da bi ocenili raven zrelosti na področju petih razsežnosti, vključenih v model CMM, se Center za zmogljivost in organizacija gostiteljica sestaneta z ustreznimi nacionalnimi deležniki iz javnega in zasebnega sektorja, na dvo- ali tri-dnevnem srečanju, da bi pripravili fokusne skupine o razsežnostih modela CMM. O vsaki razsežnosti vsaj dvakrat razpravljajo različne skupine deležnikov. Ta del predstavlja predhodno zbiranje podatkov za poznejšo oceno.

Način ali prikaz rezultatov

Model CMM zagotavlja pregled ravni zrelosti vsake države s pomočjo polarnega grafikona, ki ga sestavlja pet razdelkov, po eden za vsako razsežnost. Vsaka razsežnost predstavlja eno petino grafičnega prikaza, pri čemer se pet ravni zrelosti za vsak dejavnik razteza navzven iz središča grafikona; kot vidimo spodaj, je „faza zagona“ najbližje središču grafikona, „dinamična faza“ pa je na obrobju.

Slika 5: Pregled rezultatov modela CMM



Standards, Organisations and Technologies	Standardi, organizacije in tehnologije
Legal Regulatory Frameworks	Pravni regulativni okviri
Cybersecurity Education, Training and Skills	Izobraževanje, usposabljanje in spretnosti na področju kibernetske varnosti
Cybersecurity Policy and Strategy	Politika in strategija za kibernetsko varnost
Cyber Culture and Society	Kibernetska kultura in družba
Responsible Disclosure	Odgovorno razkritje
Cybersecurity market place	Trg kibernetske varnosti
Cryptographic Controls	Kriptografske kontrole
Technical Security Controls	Nadzor tehnične varnosti
Software Quality	Kakovost programske opreme
Internet Infrastructure Resilience	Odpornost internetne infrastrukture
Adherence to Standards	Upoštevanje standardov
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formalni in neformalni okviri sodelovanja za boj proti kibernetski kriminaliteti
Criminal Justice System	Kazenskopravni sistem
Legal Frameworks	Pravni okviri
Framework for Professional Training	Okvir za poklicno usposabljanje
Framework for Education	Okvir za izobraževanje
Awareness Raising	Ozaveščanje

Media and Social Medai	Mediji in družbeni mediji
Reporting Mechanisms	Mehanizmi poročanja
User Understanding of Personal Information Protection Online	Razumevanje uporabnikov glede varstva osebnih podatkov na spletu
Trust and Confidence on the Internet	Zaupanje in samozavest na internetu
Cybersecurity Mind-set	Miselna naravnanost h kibernetski varnosti
Communications Redundancy	Komunikacijska redundanca
Cyber Defence Consideration	Obravnava kibernetske obrambe
Crisis Management	Krizno upravljanje
CI Protection	Zaščita kritične infrastrukture
Incident Response	Odzivanje na incidente
National Cybersecurity Strategy	Nacionalna strategija za kibernetsko varnost

Svetovni center za zmogljivosti na področju kibernetske varnosti, Oxford Martin School, Univerza v Oxfordu, 2017.

A.2 Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2)

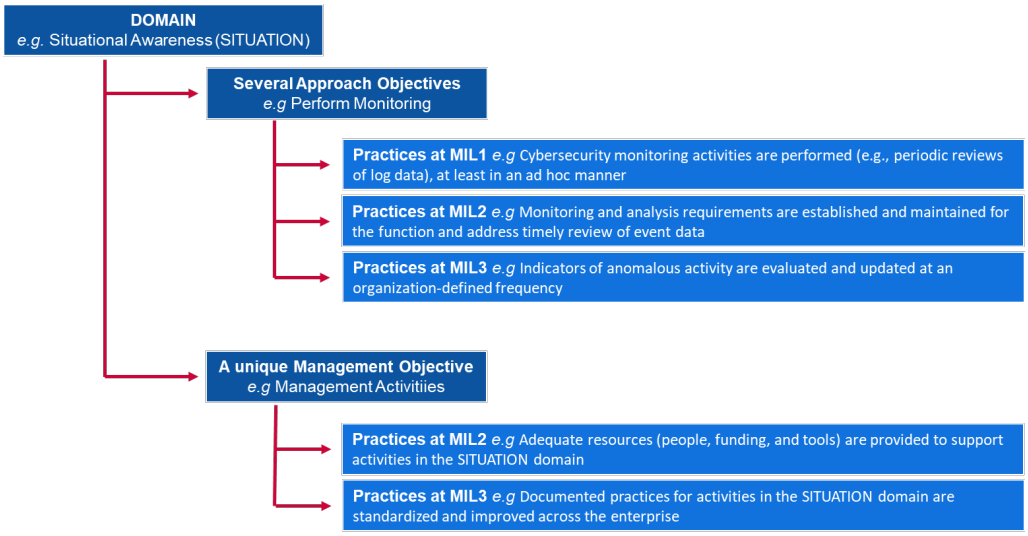
Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2) je razvilo ameriško ministrstvo za energijo v sodelovanju s strokovnjaki iz zasebnega in javnega sektorja. Cilj centra za zmogljivost je organizacijam vseh sektorjev, vrst in velikosti pomagati pri ocenjevanju in izboljšanju njihovih programov za kibernetsko varnost ter krepitvi njihove operativne odpornosti. Model C2M2 se osredotoča na izvajanje in upravljanje praks na področju kibernetske varnosti, povezanih z informacijami, informacijskimi tehnologijami (IT) in operativnimi tehnologijami (OT) ter okolji, v katerih delujejo. Model C2M2 modele zrelosti opredeljuje kot: „sklop značilnosti, atributov, kazalnikov ali vzorcev, ki predstavljajo zmogljivost in napredovanje v določeni disciplini“. Model C2M2 je bila prvič izveden leta 2014 in revidiran leta 2019.

Atributi/razsežnosti

Model C2M2 obravnava **deset področij**, ki predstavljajo logično združevanje praks na področju kibernetske varnosti. Vsak sklop praks predstavlja dejavnosti, ki jih organizacija lahko izvaja za vzpostavitev in zrelost zmogljivosti na tem področju. Vsako področje je nato povezano z **edinstvenim ciljem upravljanja** in **več cilji pristopa**. V okviru ciljev pristopa in upravljanja je navedenih **več praks**, ki podrobno opisujejo institucionalizirane dejavnosti.

Razmerje med tema pojmoma je povzeto v nadaljevanju:

Slika 6: Primer s kazalnikom modela C2M2



Domain eg Situational Awareness (SITUATION)	**Področje**, npr. zavedanje o razmerah (SITUACIJA)
Several Approaches Objectives e.g. Perform Monitoring	**Več ciljev pristopa**, npr. izvajanje spremljanja
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 MIL1**, npr. dejavnosti spremljanja kibernetske varnosti (npr. redni pregledi podatkov o dnevnikih) se izvajajo vsaj v ad hoc obliki
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Prakse na MIL2**, npr. zahteve za spremljanje in analizo se vzpostavijo in vzdržujejo za delovanje in pravočasno pregledovanje podatkov o dogodkih.
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Prakse na MIL3**, npr. kazalniki nepravilne dejavnosti se vrednotijo in posodabljajo tako pogosto, kot določi organizacija.
A unique Management Objectve e.g. Management Activities	Edinstveni cilj upravljanja, npr. dejavnosti upravljanja
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Prakse na MIL2**, npr. zagotavljajo se ustrezni viri (ljudje, financiranje in orodja) za podporo dejavnostim na področju SITUACIJA
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Prakse na MIL3**, npr. dokumentirane prakse za dejavnosti na področju SITUACIJA so standardizirane in izboljšane v celotnem podjetju.

Deset področij modela:

i obvladovanje tveganj (TVEGANJE);
ii upravljanje sredstev, sprememb in konfiguracij (SREDSTVA);
iii upravljanje identitete in dostopa (DOSTOP);
iv obvladovanje groženj in ranljivosti (GROŽNJE);
v zavedanje o razmerah (SITUACIJA);
vi odziv na dogodke in incidente (ODZIV);
vii upravljanje dobavne verige in zunanje odvisnosti (ODVISNOSTI);
viii upravljanje delovne sile (DELOVNA SILA);
ix arhitektura kibernetske varnosti (ARHITEKTURA);
x upravljanje programa za kibernetsko varnost (PROGRAM).

Ravni zrelosti

Pri modelu C2M2 se uporabljajo **4 ravni zrelosti** (imenovane ravni kazalnika zrelosti – MIL (Maturity Indicator Levels)) za določitev dvojnega napredovanja zrelosti: napredovanje na področju pristopa in napredovanje na področju upravljanja. Ravni zrelosti so od MIL0 do MIL3 in naj bi se uporabljale neodvisno pri vsakem področju.

- **MIL0 (raven zrelosti 0):** Prakse se ne izvajajo.
- **MIL1 (raven zrelosti 1):** Začetne prakse se izvajajo, vendar so lahko ad hoc narave.
- **MIL2 (raven zrelosti 2):** Značilnosti upravljanja:
  - prakse so dokumentirane;
  - za podporo procesu so na voljo ustrezna sredstva;
  - osebje, ki izvaja prakse, ima ustrezne spretnosti in znanje;
  - dodelijo se odgovornosti in pooblastila za izvajanje praks.

  Značilnost pristopa:
  - Prakse so bolj popolne ali naprednejše kot pri MIL1.

- **MIL3 (raven zrelosti 3):** Značilnosti upravljanja:
  - dejavnosti so usmerjane s strani politik (ali drugih organizacijskih direktiv);
  - cilji uspešnosti za dejavnosti na področju se določijo in spremljajo, da bi sledili dosežkom;
  - dokumentirane prakse za dejavnosti na področju so standardizirane in izboljšane v celotnem podjetju.

  Značilnost pristopa:
  - Prakse so bolj popolne ali naprednejše kot pri MIL2.

Metoda ocenjevanja

Model C2M2 je zasnovan za uporabo z **metodologijo samoocenjevanja** in naborom orodij (na voljo na zahtevo), da lahko organizacija izmeri in izboljša svoj program za kibernetsko varnost. Samoocenjevanje z uporabo nabora orodij se lahko zaključi v enem dnevu, vendar bi se lahko nabor orodij prilagodil strožjemu ocenjevanju. Poleg tega se lahko model C2M2 uporabi za usmerjanje razvoja novega programa za kibernetsko varnost.

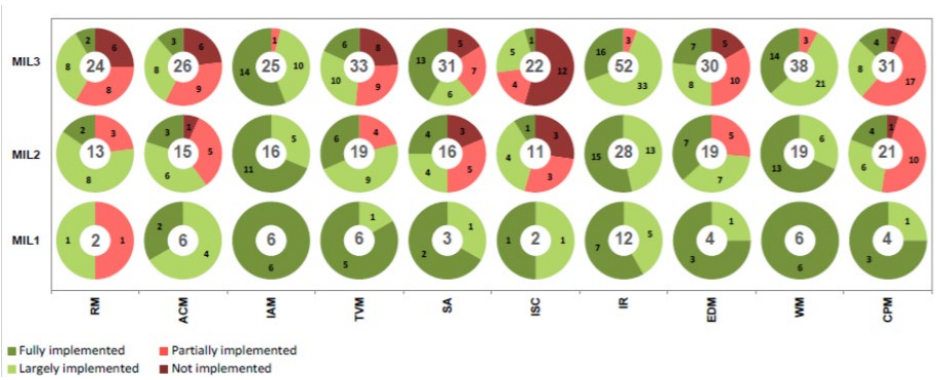
Vsebina modela je predstavljena na visoki ravni abstrakcije, tako da jo lahko interpretirajo organizacije različnih vrst, struktur, velikosti in različne industrije. Široka uporaba modela v sektorju lahko predstavlja podporo primerjalni analizi zmogljivosti sektorja na področju kibernetske varnosti.

Način ali prikaz rezultatov

Model C2M2 vsebuje poročilo o točkovanju na podlagi vrednotenja, ki je pripravljeno na podlagi rezultatov raziskave. V poročilu so rezultati predstavljeni z dveh vidikov: z vidika ciljev, ki prikazuje praktične odgovore na vprašanja za vsako področje in njegove cilje, ter z vidika področja, ki prikazuje odgovore za vsa področja in ravni zrelosti. Oba vidika temeljita na sistemu prikaza, za katerega so značilni tortni grafikoni (ali „krofi“), en graf na odgovor, in mehanizem točkovanja v obliki semaforja. Kot je prikazano na Sliki 7, rdeči segmenti v tortnih grafikonih prikazujejo število vprašanj, ki so prejela odgovore „se ne izvaja“ (temno rdeča) ali „se delno izvaja“ (svetlo rdeča). Zeleni segmenti prikazujejo število vprašanj, ki so prejela odgovore „se v veliki meri izvaja“ (svetlo zelena) ali „se v celoti izvaja“ (temno zelena).

Slika 7 prikazuje primer preglednico z rezultati, ki se izdela na koncu ocenjevanja zrelosti. Na osi X je deset področij modela C2M2, na osi Y pa ravni zrelosti (MIL). Če na grafu pogledamo področje obvladovanje tveganj (RM), je mogoče opaziti tri tortne grafikone, kjer vsak ustreza eni ravni zrelosti: MIL1, MIL2 in MIL3. Za področje RM (obvladovanje tveganj) je v grafu poudarjeno, da je treba oceniti dve postavki, da bi dosegli prvo raven zrelosti, tj. MIL1. V tem primeru je ena postavka prejela rezultat „se v veliki meri izvaja“ in ena rezultat „se delno izvaja“. Za drugo raven zrelosti (MIL2) je v modelu predvideno, da se ovrednoti 13 postavk. Dve od teh 13 postavk spadata na prvo raven ali MIL1, 11 pa jih spada na drugo raven ali MIL2. Enako velja za tretjo raven ali MIL3.

Slika 7: Model C2M2 – primer pregledne slike področja



Fully implemented	Izvedeno v celoti
Largely implemented	Večinoma izvedeno

Partially implemented	Delno izvedeno
Not implemented	Ni izvedeno
MIL1	MIL1 (RAVEN 1)
MIL2	MIL2 (RAVEN 2)
MIL3	MIL3 (RAVEN 3)
RM	obvladovanje tveganj (TVEGANJE)
ACM	upravljanje sredstev, sprememb in konfiguracij (SREDSTVA)
IAM	upravljanje identitete in dostopa (DOSTOP)
TVM	obvladovanje groženj in ranljivosti (GROŽNJE)
SA	zavedanje o razmerah (SITUACIJA)
ISC	ISC
IR	odziv na incidente (ODZIV)
EDM	upravljanje zunanje odvisnosti (ODVISNOSTI)
WM	upravljanje delovne sile (DELOVNA SILA)
CPM	upravljanje programa za kibernetsko varnost (PROGRAM)

Vir: U.S. Department of Energy, Office of electricity delivery and energy reliability (Ameriško ministrstvo za energijo, Urad za dobavo električne energije in zanesljivost oskrbe z energijo), 2015.

A.3 Okvir za izboljšanje kibernetske varnosti kritične infrastrukture

Okvir za izboljšanje kibernetske varnosti kritične infrastrukture je bil razvit v okviru nacionalnega inštituta za standarde in tehnologijo (NIST). Osredotoča se na usmerjanje dejavnosti na področju kibernetske varnosti in obvladovanje tveganj v organizaciji. Namenjen je vsem vrstam organizacij, ne glede na velikost, stopnjo tveganja na področju kibernetske varnosti ali izpopolnjenost kibernetske varnosti. Ker je to okvir in ne model, je zasnovan drugače kot prej analizirani modeli.

Okvir je sestavljen iz treh delov: jedro okvira, stopnje izvajanja in profili okvira:

- **Jedro okvira** je sklop dejavnosti na področju kibernetske varnosti, želenih rezultatov in veljavnih sklicevanj, ki so skupna vsem sektorjem kritične infrastrukture. Te so podobne atributom ali razsežnostim, ki jih najdemo v zrelostnih modelih zmogljivosti na področju kibernetske varnosti.
- **Stopnje izvajanja okvira** (v nadaljnjem besedilu: „stopnje“) zagotavljajo kontekst o tem, kako organizacija dojema tveganje na področju kibernetske varnosti, in o postopkih, ki so vzpostavljeni za obvladovanje tega tveganja. Stopnje, ki segajo od delnega izvajanja (stopnja 1) do prilagodljivega izvajanja (stopnja 4), opisujejo naraščajočo stopnjo natančnosti in izpopolnjenosti praks obvladovanja tveganj na področju kibernetske varnosti. Stopnje ne predstavljajo ravni zrelosti, temveč so namenjene podpori odločanju na ravni organizacije o tem, kako obvladovati tveganja na področju kibernetske varnosti, ter o tem, katere razsežnosti organizacije so pomembnejše in bi lahko prejele dodatna sredstva (vire).
- **Profil okvira** („profil“) predstavlja rezultate, ki temeljijo na poslovnih potrebah, ki jih je organizacija izbrala iz kategorij in podkategorij znotraj okvira. Profil je mogoče opredeliti glede na uskladitev standardov, smernic in praks z jedrom okvira v posameznem scenariju izvajanja. Profili se lahko uporabijo za opredelitev priložnosti za izboljšanje kibernetske varnosti, tako da primerjamo profil „trenutno“ (stanje „kot je“ – obstoječe stanje) s profilom „cilj“ (stanje „ki bo“ – prihodnje stanje).

Jedro okvira

Jedro okvira je sestavljeno iz petih **funkcij**. Če se te funkcije obravnavajo skupaj, zagotavljajo pomemben strateški pregled življenjskega cikla organizacije v zvezi z obvladovanjem tveganja na področju kibernetske varnosti. V jedru okvira so nato opredeljene osnovne ključne **kategorije** in **podkategorije** za vsako funkcijo, ki se ujemajo s primerom informativnih referenc, kot so obstoječi standardi, smernice in prakse za vsako podkategorijo.

Funkcije in kategorije so podrobno opisane v nadaljevanju:

i **Opredelitev**: razvoj razumevanja znotraj organizacije, na kakšne načine je mogoče obvladovati tveganja na področju kibernetske varnosti za sisteme, ljudi, sredstva, podatke in zmogljivosti.
   - Podkategorije: upravljanje sredstev, poslovno okolje, upravljanje, ocena tveganja in strategija obvladovanja tveganj.

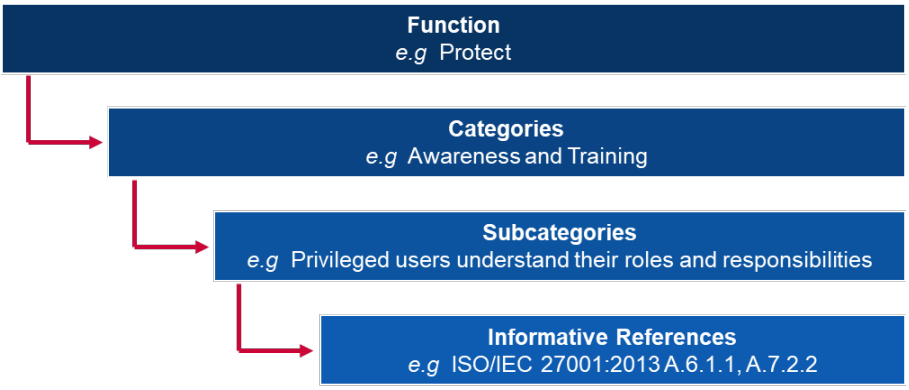
ii **Zaščita**: razvoj in izvajanje ustreznih zaščitnih ukrepov, da bi zagotovili izvajanje ključnih storitev.
   - Podkategorije: upravljanje identitete in nadzor dostopa, ozaveščanje in usposabljanje, varnost podatkov; procesi in postopki za varstvo podatkov, vzdrževanje in zaščitna tehnologija.

iii **Odkrivanje**: razvoj in izvajanje ustreznih dejavnosti za opredelitev dogodka na področju kibernetske varnosti.
   - Podkategorije: anomalije in dogodki, stalno spremljanje varnosti in postopki odkrivanja.

iv **Odzivanje**: razvoj in izvajanje ustreznih dejavnosti za ukrepanje v zvezi z odkritim kibernetskim incidentom.
   - Podkategorije: načrtovanje odzivanja, komunikacije, analiza, blažitev in izboljšave.

v **Obnovitev**: razvoj in izvajanje ustreznih dejavnosti za vzdrževanje načrtov za odpornost in ponovno vzpostavitev vseh zmogljivosti ali storitev, ki so bile oslabljene zaradi kibernetskega incidenta.
   - Podkategorije: načrt za vnovično vzpostavitev delovanja, izboljšave in komunikacije.

Slika 8: Primer okvira za izboljšanje kibernetske varnosti kritične infrastrukture



Function e.g Project	**Funkcija** npr. projekt
Categories e.g Awarness and Training	**Kategorije** npr. ozaveščanje in usposabljanje
Subcategories e.g Privileged useres understand their roles and responsibilities	**Podkategorije** npr. prednostni uporabniki razumejo svoje vloge in odgovornosti
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informativne reference** npr. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Stopnje

Okvir za izboljšanje kibernetske varnosti kritične infrastrukture temelji na **4 stopnjah,** od katerih je vsaka opredeljena na treh oseh: postopek obvladovanja tveganj, program integriranega obvladovanja tveganj in zunanja udeležba. Stopnje se ne štejejo za ravni zrelosti, temveč predstavljajo okvir, ki organizacijam zagotavlja kontekstualizacijo njihovih pogledov na tveganje na področju kibernetske varnosti ter postopke, ki so vzpostavljeni za obvladovanje tega tveganja.

- **Stopnja 1: Delno**
  - **Proces obvladovanja tveganj**: organizacijske prakse obvladovanja tveganj na področju kibernetske varnosti niso formalizirane, tveganja pa se obvladujejo na ad hoc način in včasih na odzivni način.

- **Integrirani program za obvladovanje tveganj**: ozaveščenost na organizacijski ravni o tveganjih na področju kibernetske varnosti je omejena. Organizacija izvaja obvladovanje tveganj na področju kibernetske varnosti neredno in za vsak primer posebej ter morda nima postopkov, ki bi omogočali izmenjavo informacij o kibernetski varnosti znotraj organizacije.
- **Zunanja udeležba**: organizacija ne razume svoje vloge v večjem ekosistemu, bodisi v zvezi s svojo odvisnostjo ali v zvezi z deležniki, ki so odvisni od nje. Organizacija se na splošno ne zaveda kibernetskih tveganj v zvezi z dobavno verigo proizvodov in storitev, ki jih zagotavlja in uporablja.

Stopnja 2: Seznanjenost s tveganji

- **Proces obvladovanja tveganj**: vodstvo odobri prakse obvladovanja tveganj, vendar jih ni mogoče opredeliti kot politiko na ravni organizacije.
- **Integrirani program za obvladovanje tveganj**: na organizacijski ravni obstaja ozaveščenost o tveganjih na področju kibernetske varnosti, vendar pristop na ravni celotne organizacije za obvladovanje tveganj na področju kibernetske varnosti še ni bil vzpostavljen. Ocena tveganja na področju kibernetske varnosti za organizacijska in zunanja sredstva se običajno ne ponavlja ali ni pogosta.
- **Zunanja udeležba**: organizacija na splošno razume svojo vlogo v večjem ekosistemu, bodisi v zvezi s svojo odvisnostjo ali v zvezi z odvisnimi deležniki, vendar ne v zvezi z obema. Poleg tega se organizacija zaveda kibernetskih tveganj v zvezi z dobavno verigo, ki so povezana s proizvodi in storitvami, ki jih zagotavlja in uporablja, vendar v zvezi s temi tveganji ne ukrepa dosledno ali formalno.

Stopnja 3: Ponovljivost

- **Proces obvladovanja tveganj**: prakse organizacije za obvladovanje tveganj so formalno potrjene in izražene kot politika. Organizacijske prakse na področju kibernetske varnosti se redno posodabljajo na podlagi uporabe postopkov obvladovanja tveganja pri spremembah na področju zahtev poslovanja/nalog ter na podlagi spreminjajočih se groženj in tehnologije.
- **Integrirani program za obvladovanje tveganj**: za obvladovanje tveganj na področju kibernetske varnosti obstaja pristop na ravni celotne organizacije. Politike, procesi in postopki, ki temeljijo na prepoznanem tveganju, so opredeljeni, izvedeni, kot je predvideno, in pregledani. Višji vodstveni delavci zagotavljajo upoštevanje kibernetske varnosti na vseh ravneh delovanja v organizaciji.
- **Zunanja udeležba**: organizacija razume svojo vlogo, odvisnosti in odvisne deležnike v večjem ekosistemu ter morda prispeva k širšemu razumevanju tveganj v skupnosti. Organizacija se zaveda kibernetskih tveganj v zvezi z dobavno verigo proizvodov in storitev, ki jih zagotavlja in uporablja.

Stopnja 4: Prilagodljivost:

- **Proces obvladovanja tveganj**: organizacija prilagodi svoje prakse na področju kibernetske varnosti na podlagi prejšnjih in sedanjih dejavnosti na področju kibernetske varnosti, vključno s pridobljenimi izkušnjami in napovednimi kazalniki.
- **Integrirani program za obvladovanje tveganj**: na ravni celotne organizacije obstaja pristop k obvladovanju tveganj na področju kibernetske varnosti, pri katerem se za obravnavo morebitnih dogodkov na področju kibernetske varnosti uporabljajo politike, procesi in postopki, ki temeljijo na prepoznanem tveganju.
- **Zunanja udeležba**: organizacija razume svojo vlogo, odvisnosti in odvisne deležnike v večjem ekosistemu ter prispeva k širšemu razumevanju tveganj v skupnosti.

Metoda ocenjevanja

Okvir za za izboljšanje kibernetske varnosti kritične infrastrukture je namenjen organizacijam, da same ocenijo svoje tveganje, da bi bila njihov pristop h kibernetski varnosti in naložbe bolj racionalna, učinkovita in koristna. Za preučitev učinkovitosti naložb mora organizacija najprej jasno poznati svoje organizacijske cilje, odnos med temi cilji ter podporne rezultate na področju kibernetske varnosti. Rezultati jedra okvira na področju kibernetske varnosti podpirajo samoocenjevanje naložbene učinkovitosti in dejavnosti na področju kibernetske varnosti.

A.4 Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2)

Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2) je leta 2018 razvila pravna fakulteta Univerze v Katarju. Model Q-C2M2 temelji na različnih obstoječih modelih, na podlagi katerih je bila oblikovana celovita metodologija ocenjevanja za izboljšanje katarskega okvira za kibernetsko varnost.

Atributi/razsežnosti

Model Q-C2M2 prevzema pristop nacionalnega inštituta za standarde in tehnologijo (NIST), ki uporablja pet osrednjih funkcij kot glavna področja modela. Pet osrednjih funkcij je mogoče uporabiti v katarskem kontekstu, saj so skupne v vseh sektorjih kritične infrastrukture, kar je pomemben element v katarskem okviru za kibernetsko varnost. Model Q-C2M2 temelji na **petih področjih**, pri čemer je vsako področje razdeljeno na več **podpodročij**, da se zajame celoten razpon zrelosti zmogljivosti na področju kibernetske varnosti.

Opis petih področij:

i **področje razumevanja** vključuje štiri podpodročja: kibernetsko upravljanje, sredstva, tveganja in usposabljanje;
ii podpodročja v okviru **področja varnosti** vključujejo varnost podatkov, tehnološko varnost, varnost nadzora dostopa, varnost komunikacij in varnost osebja;
iii **področje izpostavljenosti** vključuje podpodročja: spremljanje, obvladovanje incidentov, odkrivanje, analize in izpostavljenost;
iv **področje odzivanja** vključuje načrtovanje odzivanja, blažitev in obveščanje o odzivanju;
v **področje vzdrževanja** vključuje načrtovanje vnovične vzpostavitve delovanja, upravljanje neprekinjenega delovanja, izboljšanje in zunanje odvisnosti.

Ravni zrelosti

Model Q-C2M2 uporablja **5 ravni zrelosti**, s katerimi se meri zrelost zmogljivosti državnega subjekta ali nedržavne organizacije na ravni osrednje funkcije. Te ravni so namenjene ocenjevanju zrelosti na petih področjih, ki so podrobno opisana v prejšnjem oddelku.

- **Začetek**: na nekaterih področjih uporablja ad hoc prakse in postopke na področju kibernetske varnosti.
- **Izvajanje**: sprejete so politike za izvajanje vseh dejavnosti na področju kibernetske varnosti v okviru posameznih področij s ciljem, da bi se izvajanje v določenem trenutku zaključilo.
- **Razvoj**: izvajajo se politike in prakse za razvoj in izboljšanje dejavnosti na področju kibernetske varnosti v okviru posameznih področij, da bi predlagali nove dejavnosti, ki jih je treba izvajati.
- **Prilagodljivost**: ponovno pregledovanje in revizija dejavnosti na področju kibernetske varnosti ter sprejem praks na podlagi napovednih kazalnikov, ki izhajajo iz preteklih izkušenj in ukrepov.
- **Agilnost**: faza prilagajanja se še nadalje izvaja z dodatnim poudarkom na agilnosti in hitrosti pri izvajanju dejavnosti na posameznih področjih.

Metoda ocenjevanja

Model Q-C2M2 je v zgodnji fazi raziskav in še ni izgrajen za izvajanje. To je okvir, ki bi se lahko uporabil za uvedbo podrobnega modela ocenjevanja za katarske organizacije v prihodnosti.

A.5 Certificiranje zrelosti na področju kibernetske varnosti (CMMC)

Model za certificiranje zrelosti na področju kibernetske varnosti (CMMC) je razvilo ameriško ministrstvo za obrambo (DoD) v sodelovanju z Univerzo Carnegie Mellon in univerzitetnim laboratorijem Johns Hopkins University Applied Physics Laboratory. Glavni cilj ameriškega

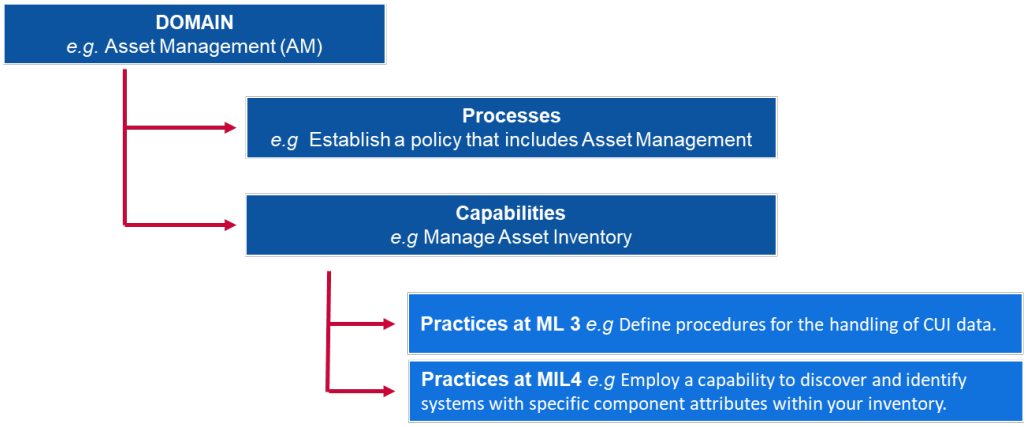
ministrstva za obrambo pri zasnovi tega modela je zaščititi informacije znotraj obrambne industrijske baze (DIB). Informacije, na katere se nanaša model CMMC, so razvrščene kot „zvezne informacije o pogodbah“, informacije, ki jih vlada zagotovi ali pridobi na podlagi pogodbe in niso namenjene za javno objavo, ali kot „nadzorovane nerazvrščene informacije“, informacije, ki zahtevajo zaščito ali nadzor nad razširjanjem v skladu z zakoni, predpisi in politikami na ravni celotne vlade. Model CMMC meri zrelost na področju kibernetske varnosti in zagotavlja najboljše prakse skupaj z elementom certificiranja, da se zagotovi izvajanje praks, povezanih s posamezno stopnjo zrelosti. Najnovejša različica modela CMMC je bila objavljena leta 2020.

Atributi/razsežnosti

Model CMMC obravnava **sedemnajst področij,** ki predstavljajo sklope procesov in zmogljivosti na področju kibernetske varnosti. Vsako področje se nato razčleni na več **procesov**, ki so podobni na vseh področjih, in na eno ali več **zmogljivosti**, ki se razvrščajo v pet ravni zrelosti. Zmogljivosti (ali zmogljivost) so nato podrobno opisane v **praksah** za vsako ustrezno raven zrelosti.

Razmerje med temi pojmi je naslednje:

Slika 9: Primer kazalnikov modela CMMC



DOMAIN e.g. Asset Management (AM)	**PODROČJE** npr. upravljanje sredstev (AM)
Processes e.g Establish a policy that includes Asset Management	**Procesi** npr. vzpostavitev politike, ki vključuje upravljanje sredstev
Capabilities e.g Manage Asset Inventory	**Zmogljivosti** npr. upravljanje inventarja sredstev
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Prakse na ravni zrelosti 3,** npr. opredelitev postopkov za ravnanje z nadzorovanimi nerazvrščenimi informacijami
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Prakse na ravni zrelosti 4,** npr. zmogljivost odkrivanja in prepoznavanja sistemov s posebnimi atributi komponent znotraj inventarja

Opis sedemnajstih področij:

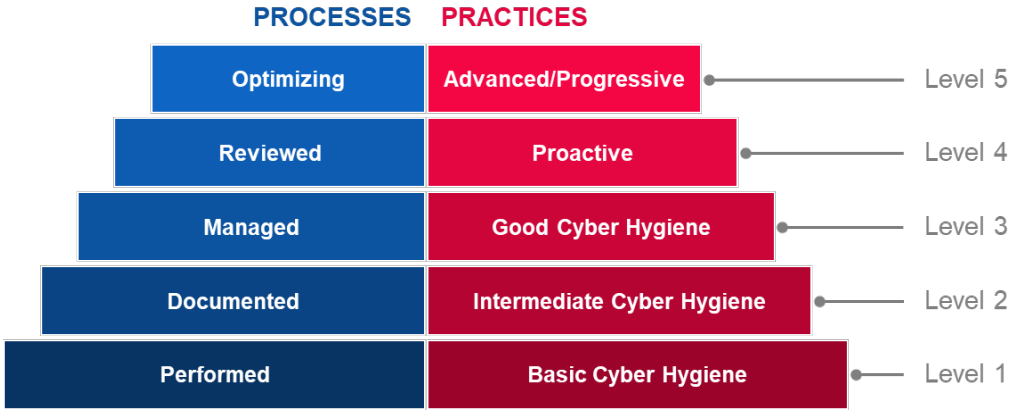
i nadzor dostopa (AC),
ii upravljanje sredstev (AM),
iii revizija in odgovornost (AU),

iv ozaveščanje in usposabljanje (AT),
v upravljanje konfiguracij (CM),
vi identifikacija in avtentikacija (IA),
vii odzivanje na incidente (IR),
viii vzdrževanje (MA),
ix zaščita medijev (MP),
x varnost osebja (PS),
xi fizično varovanje (PE),
xii sanacija (RE),
xiii obvladovanje tveganj (RM),
xiv ocena varnosti (CA),
xv zavedanje o razmerah (SA),
xvi zaščita sistema in komunikacij (SC) in
xvii celovitost sistema in informacij (SI).

Ravni zrelosti

Model CMMC uporablja **5 ravni zrelosti**, ki so opredeljene na podlagi procesov in praks. Da bi organizacija dosegla določeno raven zrelosti po modelu CMMC, mora izpolniti predpogoje za postopke in prakse na tej ravni. To pomeni tudi izpolnjevanje predpogojev za vse ravni, ki so nižje od navedene.

Slika 10: Ravni zrelosti po modelu CMMC



PROCESSES	PROCESI
Optimizing	Optimizirani
Reviewed	Pregledani
Managed	Upravljani
Documented	Dokumentirani
Performed	Se izvajajo
PRACTICES	PRAKSE
Advanced/Progressive	Napredne/progresivne
Proactive	Proaktivne
Good Cyber Hygiene	Dobra kibernetska higiena
Intermediate Cyber Hygiene	Srednja kibernetska higiena
Basic Cyber Hygiene	Osnovna kibernetska higiena
Level 5	Raven 5
Level 4	Raven 4
Level 3	Raven 3
Level 2	Raven 2:
Level 1	Raven 1:

- **Raven 1:**
  - **Procesi – se izvajajo:** ker lahko organizacija te prakse izvaja le priložnostno (ad hoc) in se lahko zanese na dokumentacijo ali ne. Zrelost procesa se za raven 1 ne ocenjuje.
  - **Prakse – osnovna kibernetska higiena**: raven 1 se osredotoča na zaščito zveznih informacij o pogodbah (FCI) in zajema le prakse, ki ustrezajo osnovnim zahtevam zaščite.
- **Raven 2:**
  - **Procesi – so dokumentirani**: raven 2 zahteva, da organizacija vzpostavi in dokumentira prakse in politike za usmerjanje izvajanja svojih prizadevanj v okviru modela CMMC. Dokumentacija o praksah posameznikom omogoča, da jih izvajajo na ponovljiv način. Organizacije razvijejo zrele zmogljivosti s pomočjo dokumentiranja svojih postopkov in nato z njihovim izvajanjem na način, kot je dokumentirano.
  - **Prakse – srednja kibernetska higiena**: raven 2 služi kot srednja raven med ravnjo 1 in ravnjo 3 in je sestavljena iz podskupine varnostnih zahtev, ki so določene v standardu NIST SP 800-171, ter praks iz drugih standardov in referenc.
- **Raven 3**
  - **Procesi – se upravljajo**: raven 3 zahteva, da organizacija pripravi, vzdržuje in financira načrt, ki prikazuje upravljanje dejavnosti za izvajanje praks. Načrt lahko vključuje informacije o poslanstvu, ciljih, projektnih načrtih, virih, potrebnem usposabljanju in sodelovanju ustreznih deležnikov.
  - **Prakse – dobra kibernetska higiena**: raven 3 se osredotoča na zaščito nadzorovanih nerazvrščenih informacij (CUI) in zajema vse varnostne zahteve, določene v standardu NIST SP 800-171, ter dodatne prakse iz drugih standardov in referenc za ublažitev nevarnosti.
- **Raven 4**
  - **Procesi – so pregledani**: raven 4 zahteva, da organizacija pregleduje in meri učinkovitost praks. Poleg merjenja učinkovitosti praks lahko organizacije na tej ravni po potrebi sprejmejo korektivne ukrepe in redno obveščajo višje ravni upravljanja o stanju ali težavah.
  - **Prakse – so proaktivne**: raven 4 se osredotoča na zaščito nadzorovanih nerazvrščenih informacij (CUI) in zajema podskupino okrepljenih varnostnih zahtev. Te prakse krepijo zmogljivosti organizacije za odkrivanje in odzivanje na spreminjajoče se taktike, tehnike in postopke ter prilagajanje nanje.
- **Raven 5**
  - **Procesi – so optimizirani**: raven 5 zahteva, da organizacija standardizira in optimizira izvajanje postopkov v organizaciji.
  - **Prakse – so napredne/proaktivne**: raven 5 se osredotoča na zaščito nadzorovanih nerazvrščenih informacij (CUI). Dodatne prakse povečujejo globino in izpopolnjenost zmogljivosti na področju kibernetske varnosti.

Metoda ocenjevanja

Model CMMC je razmeroma mlad model, ki je bil dokončan v prvem četrtletju leta 2020. Doslej še ni bil uporabljen v nobeni organizaciji. Kljub temu pogodbeni izvajalci ameriškega ministrstva za obrambo (DoD) pričakujejo, da se bodo za izvedbo revizij obrnili na certificirane zunanje revizorje. Ameriško ministrstvo za obrambo (DoD) od svojih pogodbenih izvajalcev pričakuje, da bodo izvajali najboljše prakse za spodbujanje kibernetske varnosti in varstva občutljivih informacij.

A.6 Zrelostni model kibernetske varnosti skupnosti (CCSMM)

Zrelostni model kibernetske varnosti skupnosti (CCSMM) je razvil Center za zagotavljanje in varnost infrastrukture, ki deluje v okviru Univerze v Teksasu (Centre for Infrastructure Assurance and Security). Cilj modela CCSMM je bolje opredeliti metode za določitev trenutnega stanja skupnosti v zvezi z njeno pripravljenostjo na področju kibernetske varnosti in zagotoviti časovni načrt, ki mu bodo skupnosti sledile pri svojih prizadevanjih za pripravo. Skupnosti, na

katere se nanaša model CCSMM, so večinoma lokalne ali državne uprave. Model CCSMM je bil zasnovan leta 2007.

Atributi/razsežnosti

Ravni zrelosti so opredeljene v okviru **6 glavnih razsežnosti**, ki zajemajo različne vidike kibernetske varnosti v skupnostih in organizacijah. Te razsežnosti so jasno opredeljene za vsako raven zrelosti (podrobno opisane na Sliki 31: Povzetek razsežnosti modela **CCSMM**). Šest glavnih razsežnosti:

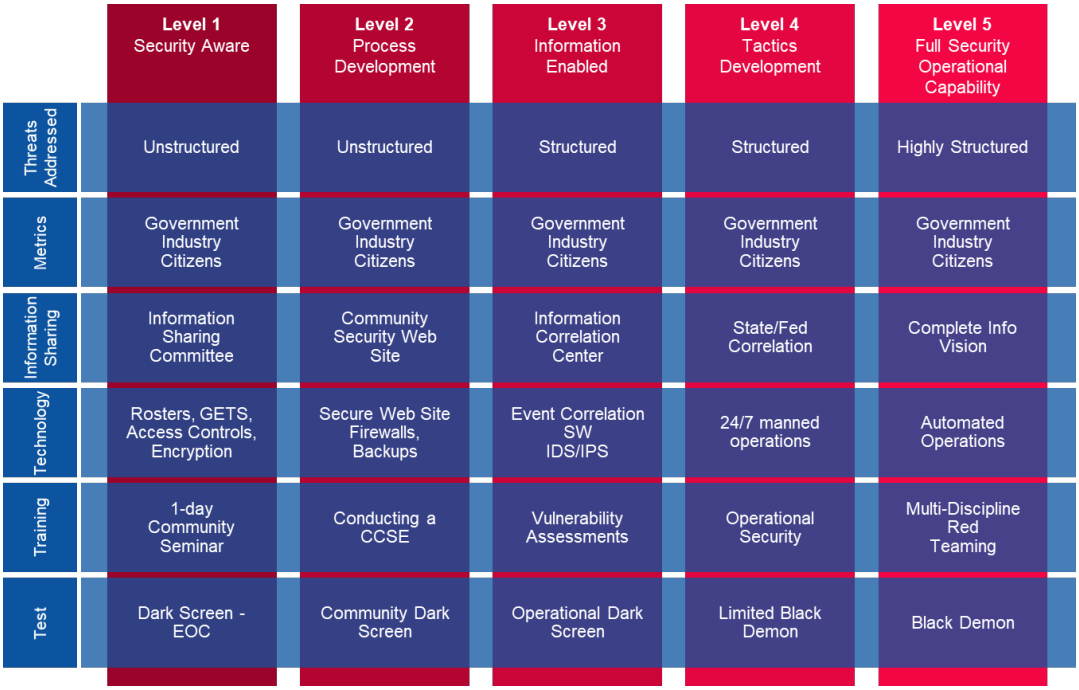
i obravnavanje groženj,
ii metrike,
iii izmenjava informacij,
iv tehnologija,
v usposabljanje in
vi preizkus.

Ravni zrelosti

Model CCSMM se opira na **5 ravni zrelosti**, ki temeljijo na glavnih vrstah groženj in dejavnosti, ki so obravnavane na določeni ravni.

- **Raven 1: Ozaveščenost glede varnosti**
  Najpomembnejša dejavnost na tej ravni je ozaveščanje posameznikov in organizacij o grožnjah, težavah in vprašanjih, ki so povezana s kibernetsko varnostjo.
- **Raven 2: Razvoj procesa**
  Raven je oblikovana za pomoč skupnostim pri vzpostavljanju in izboljševanju varnostnih postopkov, ki so potrebni za učinkovito obravnavo vprašanj na področju kibernetske varnosti.
- **Raven 3: Omogočena informiranost**
  Namen je izboljšati mehanizme za izmenjavo informacij znotraj skupnosti, da bi lahko skupnost učinkovito povezala na videz različne informacije.
- **Raven 4: Razvoj taktike**
  Elementi na tej ravni so zasnovani za razvoj boljših in bolj proaktivnih metod za odkrivanje napadov in odzivanje nanje. Na tej ravni bi morala biti vzpostavljena večina metod za preprečevanje.
- **Raven 5: Polna varnostna operativna zmogljivost**
  Ta raven predstavlja tiste elemente, ki bi morali biti vzpostavljeni, če želi neka organizacija biti v celoti operativno pripravljena na spopadanje s katero koli vrsto kibernetske grožnje.

Slika 31: Povzetek razsežnosti modela CCSMM po ravneh



Level 1 Security Aware	Raven 1 Ozaveščenost glede varnosti
Level 2 Process Development	Raven 2 Razvoj procesa
Level 3 Information Enabled	Raven 3 Omogočena informiranost
Level 4 Tactics Development	Raven 4 Razvoj taktike
Level 5 Full Security Operational Capability	Raven 5 Polna varnostna operativna zmogljivost
Threats Addressed	Obravnavanje groženj
Metrics	Metrike
Information sharing	Izmenjava informacij
Technology	Tehnologija
Training	Usposabljanje
Test	Test
Unstructured	Nestrukturirano
Governement Industry Citizens	Uprava Industrija Državljani
Information Sharing Committee	Odbor za izmenjavo informacij
Rosters, GETS, Assess Controls, Encryption	Seznami, GETS (vladna služba za urgentne telekomunikacije), ocenjevalni pregledi, šifriranje
1-dat Community Seminar	enodnevni seminar za skupnost
Dark Screen – EOC	Test „Dark Screen – EOC“
Unstructured	Nestrukturirano
Governement Industry Citizens	Uprava Industrija Državljani
Community Security Web site	Spletna stran o varnosti skupnosti
Secure Web Site Firewalls, Backups	Varni spletni požarni zidovi, varnostne kopije
Conudcting a CCSE	Izvajanje tečaja CCSE (certificirani strokovnjak za varnost)
Community Dark Screen	Test „Community Dark Screen“
Structured	Strukturiran
Governement Industry Citizens	Uprava Industrija Državljani
Information Correlation Center	Informacijski center za korelacijo

Event Correlation SW IDS/IPS	Tehnologija „Event Correlation SW IDS/IPS“ (Sistem za preprečevanje vdorov ipd.)
Vulnerability Assessment	Ocena ranljivosti
Operational Dark Screen	Test „Operational Dark Screen“
Structured	Strukturiran
Governement Industry Citizens	Uprava Industrija Državljani
State/Fed Correlation	Korelacija med državo in zvezno državo
24/7 manned operations	Operacije 24/7 z osebjem
Operational Security	Operativna varnost
Limited Black Demon	Test „Limited Black Demon“
Highly Structured	Visoko strukturiran
Governement Industry Citizens	Uprava Industrija Državljani
Complete Info Vision	Popoln pregled informacij
Automated Operations	Avtomatizirane operacije
Multi-Discipline Red Teaming	Večdisciplinarni „Red Teaming“
Black Demon	Simulacija „Black Demon“

Metoda ocenjevanja

Model CCSMM naj bi kot metodologijo ocenjevanja uporabljale skupnosti ob sodelovanju državnih in zveznih organov kazenskega pregona. Njegov namen je pomagati skupnosti pri opredelitvi tega, kar je najbolj pomembno, pri opredelitvi najverjetnejših ciljev in tega, kaj je treba zaščititi (in v kakšnem obsegu). Ob upoštevanju teh ciljev se lahko pripravijo načrti, da se vsak vidik skupnosti dvigne na zahtevano raven zrelosti na področju kibernetske varnosti. Posebni podatki, ki se zberejo v okviru modela CCSMM, pomagajo opredeliti cilje različnih preskusov in vaj, ki se lahko uporabijo za merjenje učinkovitosti vzpostavljenih programov.

A.7 Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (ISMM)

Zrelostni model informacijske varnosti (ISMM) je bil razvit na Visoki šoli za računalništvo in inženiring (College of Computer Sciences and Engineering) na Univerzi King Fahd University of Petroleum and Minerals v Savdski Arabiji. Predlaga nov zrelostni model zmogljivosti za merjenje izvajanja ukrepov na področju kibernetske varnosti. Cilj modela ISMM je organizacijam omogočiti merjenje njihovega napredka pri izvajanju v daljšem časovnem obdobju, tako da vsakokrat uporabijo isti merilni instrument, da bi ohranile želeni položaj glede tveganja. Model ISMM je bila razvit leta 2017.

Atributi/razsežnosti

Model ISMM temelji na obstoječih ocenjenih področjih okvira NIST in dodaja razsežnost ocene skladnosti. Tako ima model **23 ocenjenih področij** za položaj organizacije glede tveganja. Seznam 23 ocenjenih področij je naslednji:

i Upravljanje sredstev
ii poslovno okolje,
iii upravljanje,
iv ocena tveganja,
v strategija obvladovanja tveganj,
vi ocena skladnosti,
vii Nadzor dostopa
viii Ozaveščenost in usposabljanje
ix varnost podatkov,

x procesi in postopki za varstvo podatkov,
xi Vzdrževanje
xii zaščitna tehnologija;
xiii anomalije in dogodki,
xiv stalno spremljanje varnosti,
xv postopki odkrivanja,
xvi načrtovanje odziva,
xvii obveščanje o odzivu,
xviii analiza odziva,
xix blažitev odziva,
xx izboljšanje odziva,
xxi načrtovanje sanacije,
xxii izboljšanje sanacije in
xxiii obveščanje o sanaciji.

Ravni zrelosti

Model ISMM temelji na **5 ravneh zrelosti**, ki žal niso podrobno opisane v razpoložljivi dokumentaciji.

- **Raven 1:** izvedeni postopek
- **Raven 2:** upravljani postopek
- **Raven 3:** vzpostavljen postopek
- **Raven 4:** predvidljiv postopek
- **Raven 5:** postopek optimizacije.

Metoda ocenjevanja

Model ISMM ne predlaga nobene posebne metodologije za izvajanje ocenjevanja za organizacije.

A.8 Model službe za notranjo revizijo za javni sektor (IA-CM)

Model službe za notranjo revizijo (IA-CM) je razvila raziskovalna fundacija Inštituta notranjih revizorjev (Institute of Internal auditors Research Foundation) za krepitev zmogljivosti in zagovorništva s pomočjo samoocenjevanja v javnem sektorju. Model IA-CM, ki je namenjen revizorjem, zagotavlja pregled samega modela skupaj z navodili za uporabo, ki so v pomoč pri uporabi modela kot orodja za samoocenjevanje.

Čeprav je model IA-CM osredotočen na zmogljivosti notranje revizije in ne na krepitev zmogljivosti na področju kibernetske varnosti, je zasnovan kot orodje za samoocenjevanje zrelosti za subjekte javnega sektorja, ki se lahko uporablja na svetovni ravni za izboljšanje procesov in učinkovitosti. Ker področje uporabe ni osredotočeno na kibernetsko varnost, atributi ne bodo analizirani. Model IA-CM je bil dokončan leta 2009.

Ravni zrelosti

Model službe za notranjo revizijo (IA-CM) vključuje **5 ravni zrelosti**, od katerih vsaka opisuje značilnosti in zmogljivosti dejavnosti notranje revizije na tisti ravni. Ravni zmogljivosti v modelu zagotavljajo načrt za nenehno izboljševanje.

- **Raven 1: Začetna**
  Ni trajnostnih, ponovljivih zmogljivosti – odvisno od individualnih prizadevanj
  - Priložnostno (ad hoc) ali nestrukturirano.
  - Posamezne enotne revizije ali pregledi dokumentov in transakcij glede točnosti in skladnosti.
  - Rezultati so odvisni od spretnosti določene osebe na tem položaju.

- Poklicne prakse niso vzpostavljene, razen tiste, ki jih zagotavljajo poklicna združenja.
- Po potrebi odobritev financiranja s strani vodstva.
- Pomanjkanje infrastrukture.
- Revizorji so verjetno del večje organizacijske enote.
- Institucionalne zmogljivosti niso razvite.

▶ **Raven 2: Infrastrukturna**
Trajnostne in ponovljive prakse in postopki

- Ključno vprašanje ali izziv za raven 2 je, kako vzpostaviti in ohranjati ponovljivost postopkov in s tem ponovljivo zmogljivost.
- Vzpostavljajo se odnosi poročanja, upravljavske in upravne infrastrukture ter strokovne prakse in procesi notranje revizije (navodila, procesi in postopki za notranjo revizijo).
- Načrtovanje revizij, ki temelji predvsem na prednostnih nalogah upravljanja.
- Nadaljnje zanašanje predvsem na spretnosti in kompetence določenih oseb.
- Delna skladnost s standardi.

▶ **Raven 3: Integrirana**
Enotno izvajanje upravljanja in poklicnih praks

- Politike, procesi in postopki notranje revizije so opredeljeni, dokumentirani in vključeni drug v drugega ter v infrastrukturo organizacije.
- Upravljanje notranje revizije in strokovne prakse so dobro uveljavljene in se enotno uporabljajo pri vseh dejavnostih notranje revizije.
- Notranja revizija se začenja usklajevati s poslovanjem organizacije in tveganji, s katerimi se sooča.
- Notranja revizija sega od izvajanja zgolj tradicionalne notranje revizije do vključevanja v skupino ter svetovanja glede uspešnosti in obvladovanja tveganj.
- Poudarek je na krepitvi skupinskega duha in zmogljivosti na področju dejavnosti službe notranje revizije ter njeni neodvisnosti in objektivnosti.
- Je na splošno v skladu s standardi.

▶ **Raven 4: Upravljana**
Vključuje informacije iz celotne organizacije za izboljšanje upravljanja in obvladovanja tveganj

- Pričakovanja službe notranje revizije in ključnih deležnikov so usklajena.
- Vzpostavljene so metrike uspešnosti za merjenje in spremljanje postopkov in rezultatov notranje revizije.
- Za službo notranje revizijo velja, da pomembno prispeva k organizaciji.
- Služba za notranjo revizijo deluje kot sestavni del upravljanja in obvladovanja tveganj organizacije.
- Služba za notranjo revizijo je dobro upravljana poslovna enota.
- Tveganja se merijo in upravljajo na kvantitativen način.
- Vzpostavljene so potrebne spretnosti in kompetence, ki omogočajo obnovo in izmenjavo znanja (v okviru službe za notranjo revizijo in po celotni organizaciji).

▶ **Raven 5: Optimizirana**
Učenje s pomočjo informacij iz organizacije in zunaj nje za nenehno izboljševanje

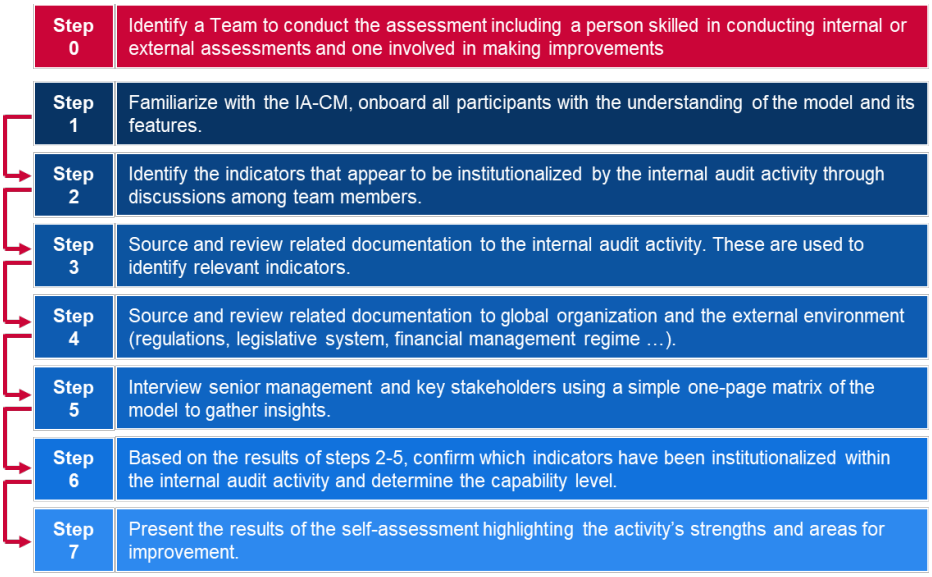
- Služba za notranjo revizijo je organizacija, ki se uči in izvaja stalne izboljšave procesov in inovacije.
- Služba za notranjo revizijo z uporabo notranjih in zunanjih informacij prispeva k doseganju strateških ciljev.
- Uspešnost na vrhunski ravni / priporočena / najboljša praksa.
- Notranja revizija je ključni del strukture upravljanja organizacije.
- Vrhunske strokovne in specializirane spretnosti.
- Individualna, skupinska in organizacijska merila uspešnosti so v celoti integrirana za
- spodbujanje izboljšav na področju uspešnosti.

Metoda ocenjevanja

Model službe za notranjo revizijo je jasno oblikovan za samoocenjevanje. Zagotavlja podrobne korake, ki jih je treba upoštevati pri uporabi modela IA-CM, in vzorčne diapozitive, ki se lahko prilagodijo. Pred začetkom samoocenjevanja je treba določiti posebno ekipo, ki vključuje vsaj

eno osebo, ki je usposobljena za izvajanje notranjih ali zunanjih ocen notranjih revizij, in eno osebo, ki sodeluje pri izboljšavah na tem področju.

Slika 12: Koraki za samoocenjevanje po modelu IC-AM



Step 0	Korak 0
Step 1	Korak 1
Step 2	Korak 2
Step 3	Korak 3
Step 4	Korak 4
Step 5	Korak 5
Step 6	Korak 6
Step 7	Korak 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Določite skupino, ki bo izvajala ocenjevanje, vključno z osebo, ki je usposobljena za izvajanje notranjih ali zunanjih ocen, in osebo, ki sodeluje pri izboljšavah.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Seznanite se z modelom IA-CM in vse udeležence seznanite z razumevanjem modela in njegovih značilnosti.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Opredelite kazalnike, za katere se zdi, da so institucionalizirani v okviru dejavnosti službe za notranjo revizijo, in sicer s pomočjo razprave med člani skupine.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Poiščite in preglejte dokumentacijo v zvezi z dejavnostjo notranje revizije. Slednja se uporablja za opredelitev ustreznih kazalnikov.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Poiščite in preglejte dokumentacijo v zvezi s celotno organizacijo in zunanjim okoljem (uredbe, zakonodajni sistem, ureditev finančnega poslovodenja ...).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Opravite razgovore z višjim vodstvom in ključnimi deležniki s pomočjo preproste

	enostranske matrike modela, da pridobite vpogled.
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 podlagi rezultatov iz korakov 2–5 potrdite, kateri kazalniki so bili institucionalizirani v okviru dejavnosti službe za notranjo revizijo, in določite raven zmogljivosti.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Predstavite rezultate samoocenjevanja, v katerih so poudarjene prednosti in področja, na katerih so potrebne izboljšave.

A.9 Svetovni indeks kibernetske varnosti (GCI)

Svetovni indeks kibernetske varnosti (GCI) je pobuda Mednarodne telekomunikacijske zveze (ITU). Njegov cilj je pregledati zavezanost h kibernetski varnosti in razmere na področju kibernetske varnosti v vseh regijah Mednarodne komunikacijske zveze: Afrika, Amerike, arabske države, azijsko-pacifiške države, SND in Evropa. V središče pozornosti postavlja države z visoko zavezanostjo in priporočljivimi praksami. Cilj svetovnega indeksa kibernetske varnosti je pomagati državam opredeliti področja, na katerih so potrebne izboljšave na področju kibernetske varnosti, in jih motivirati, da sprejmejo ukrepe za izboljšanje njihovega razvrščanja, s čimer prispevajo k zvišanju splošne ravni kibernetske varnosti po vsem svetu.

Ker svetovni indeks kibernetske varnosti ni model zrelosti, za razvrščanje in primerjavo globalnih zavez držav in regij glede kibernetske varnosti ne uporablja ravni zrelosti, temveč oceno.

Atributi/razsežnosti

Svetovni indeks kibernetske varnosti temelji na petih stebrih globalne agende za kibernetsko varnost (GCA). Ti stebri tvorijo pet podindeksov in vsak vključuje sklop kazalnikov. Pet stebrov in spremljajoči kazalniki so naslednji:

i **Pravni:** ukrepi, ki temeljijo na obstoju pravnih institucij in okvirov za kibernetsko varnost in kibernetsko kriminaliteto.
- Zakonodaja na področju kibernetske kriminalitete
- Predpisi na področju kibernetske varnosti
- Zakonodaja na področju zajezitve/omejevanja neželene elektronske pošte

ii **Tehnični**: ukrepi, ki temeljijo na obstoju tehničnih institucij in okvirov za kibernetsko varnost.
- CERT/CIRT/CSRIT
- Okvir za izvajanje standardov
- Organ za standardizacijo
- Tehnični mehanizmi in zmogljivosti, uporabljene za obravnavo neželene elektronske pošte
- Uporaba oblaka za namene kibernetske varnosti
- Mehanizmi za zaščito otrok na spletu

iii **Organizacijski**: ukrepi, ki temeljijo na obstoju institucij za usklajevanje politik in strategij za razvoj kibernetske varnosti na nacionalni ravni.
- Nacionalna strategija za kibernetsko varnost
- Pristojna agencija
- Kibernetska varnost

iv **Krepitev zmogljivosti:** ukrepi, ki temeljijo na obstoju raziskav in razvoja, programov izobraževanja in usposabljanja, certificiranih strokovnjakov in agencij javnega sektorja, ki spodbujajo krepitev zmogljivosti.
- Kampanje ozaveščanja javnosti
- Okvir za certificiranje in akreditacijo strokovnjakov za kibernetsko varnost
- Tečaji strokovnega usposabljanja na področju kibernetske varnosti
- Izobraževalni programi ali akademski učni načrti na področju kibernetske varnosti
- Programi raziskav in razvoja na področju kibernetske varnosti

- Spodbujevalni mehanizmi

v **Sodelovanje**: ukrepi, ki temeljijo na obstoju partnerstev, okvirov sodelovanja in mrež za izmenjavo informacij.
  - Dvostranski sporazumi
  - Večstranski sporazumi
  - Sodelovanje v mednarodnih forumih/združenjih
  - Javno-zasebna partnerstva
  - Partnerstva med agencijami in znotraj njih
  - Najboljše prakse

Metoda ocenjevanja

Svetovni indeks kibernetske varnosti je orodje za samoocenjevanje, zgrajeno na podlagi vprašalnika[30], ki vsebuje binarna, vnaprej kodirana in odprta vprašanja. Uporaba binarnih odgovorov odpravlja vrednotenje, ki temelji na mnenjih, in morebitno pristranskost do nekaterih vrst odgovorov. Vnaprej kodirani odgovori prihranijo čas in omogočajo natančnejšo analizo podatkov. Poleg tega preprosta dihotomna lestvica omogoča hitrejše in bolj zapleteno ocenjevanje, saj ne zahteva dolgih odgovorov, kar pospešuje in racionalizira postopek zagotavljanja odgovorov in nadaljnje ocenjevanje. Respondent mora potrditi le prisotnost ali odsotnost določenih predhodno opredeljenih rešitev na področju kibernetske varnosti. Mehanizem spletne ankete, ki se uporablja za zbiranje odgovorov in nalaganje ustreznega gradiva, omogoča izvleček dobrih praks in sklop tematskih kvalitativnih ocen, ki jih opravi skupina strokovnjakov.

Splošni postopek svetovnega indeksa kibernetske varnosti se izvaja na naslednji način:

- Vsem udeležencem se pošlje vabilo, v katerem so obveščeni o pobudi in naprošeni, da sporočijo kontaktno točko, ki bo odgovorna za zbiranje vseh ustreznih podatkov in izpolnjevanje spletnega vprašalnika. Mednarodna telekomunikacijska zveza (ITU) v času trajanja spletne raziskave uradno povabi odobreno kontaktno točko, da odgovori na vprašalnik.
- Zbiranje primarnih podatkov (za države, ki ne izpolnijo vprašalnika):
  - ITU pripravi prvi osnutek odgovora na vprašalnik z uporabo javno dostopnih podatkov in spletnih raziskav;
  - osnutek vprašalnika se pošlje kontaktnim točkam v pregled;
  - kontaktne točke izboljšajo natančnost in nato vrnejo osnutek vprašalnika;
  - popravljeni osnutek vprašalnika se pošlje vsaki kontaktni točki v končno odobritev;
  - potrjeni vprašalnik se uporablja za analizo, točkovanje in razvrstitev.
- Zbiranje sekundarnih podatkov (za države, ki odgovorijo na vprašalnik):
  - ITU opredeli morebitne manjkajoče odgovore, spremno dokumentacijo, povezave itd.;
  - kontaktna točka po potrebi izboljša natančnost odgovorov;
  - popravljeni osnutek vprašalnika se pošlje vsaki kontaktni točki v končno odobritev;
  - potrjeni vprašalnik se uporablja za analizo, točkovanje in razvrstitev.

A.10 Indeks kibernetske moči (CPI)

Indeks kibernetske moči (CPI) je leta 2011 pripravilo podjetje Economist Intelligence Unit v okviru raziskovalnega programa, ki ga je sponzoriralo podjetje Booz Allen Hamilton. Indeks kibernetske moči je „dinamični kvantitativni in kvalitativni model [...], ki meri posebne lastnosti

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

kibernetskega okolja v okviru štirih dejavnikov kibernetske moči: pravni in regulativni okvir, gospodarski in družbeni kontekst, tehnološka infrastruktura in uporaba v industriji, ki preučuje digitalni napredek v ključnih industrijah“[31]. Cilj indeksa kibernetske moči je primerjati sposobnost držav skupine G20 v obrambi pred kibernetskimi napadi in pri uvajanju potrebne digitalne infrastrukture za uspešno in varno gospodarstvo. Primerjalna analiza, ki jo zagotavlja indeks kibernetske moči, se osredotoča na 19 držav skupine G20 (brez EU). Indeks nato ponuja razvrstitev držav za vsak kazalnik.

Atributi/razsežnosti

Indeks kibernetske moči (CPI) temelji na štirih dejavnikih kibernetske moči. Vsaka kategorija se nato meri z več kazalniki, da se vsaki državi dodeli posebna ocena. Kategorije in stebri so naslednji:

i **Pravni in regulativni okvir**
- Zavezanost vlade h kibernetskemu razvoju
- Politike kibernetske zaščite
- Kibernetska cenzura (ali njeno pomanjkanje)
- Politična učinkovitost
- Varstvo intelektualne lastnine

ii **Gospodarski in družbeni kontekst**
- Ravni izobrazbe
- Tehnične spretnosti
- Odprtost trgovine
- Stopnja inovativnosti v poslovnem okolju

iii **Tehnološka infrastruktura**
- Dostop do informacijske in komunikacijske tehnologije
- Kakovost informacijske in komunikacijske tehnologije
- Cenovna dostopnost informacijske in komunikacijske tehnologije
- Poraba za informacijsko tehnologijo
- Število varnih strežnikov

iv **Uporaba v industriji**
- Pametna omrežja
- E-zdravje
- E-trgovanje
- Inteligentni promet
- E-uprava

Metoda ocenjevanja

Indeks kibernetske moči je kvantitativen in kvalitativen model točkovanja. Ocenjevanje je izvedlo podjetje Economist Intelligence Unit z uporabo kvantitativnih kazalnikov iz razpoložljivih statističnih virov in pripravo ocen, kadar podatkov ni bilo. Glavni uporabljeni viri so podjetje Economist Intelligence Unit, Organizacija Združenih narodov za izobraževanje, znanost in kulturo (UNESCO), Mednarodna telekomunikacijska zveza (ITU) in Svetovna banka.

A.11 Indeks kibernetske moči (CPI)

V tem oddelku so povzete glavne ugotovitve iz analize obstoječih zrelostnih modelov. Preglednica 5: Pregled analiziranih zrelostnih modelov vsebuje pregled glavnih značilnosti posameznega modela v skladu s spremenjenim Beckerjevim modelom. Preglednica 6 Primerjava ravni zrelosti prikazuje višjo raven opredelitev ravni zrelosti analiziranih modelov. Preglednica 7 vsebuje pregled razsežnosti ali atributov, uporabljenih v posameznem modelu.

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

Preglednica 5: Pregled analiziranih zrelostnih modelov

Ime modela	Institucija	Namen	Cilj	Število ravni	Število atributov	Metoda ocenjevanja	Prikaz rezultatov
Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM)	Svetovni center za zmogljivosti na področju kibernetske varnosti Univerza v Oxfordu	Povečanje obsega in učinkovitosti krepitve zmogljivosti na področju kibernetske varnosti na mednarodni ravni	Države	5	5 glavnih razsežnosti	sodelovanje z lokalnimi organizacijami za izpopolnitev modela pred njegovo uporabo v nacionalnem kontekstu	polarni (radarski) grafikon s 5 razdelki
Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2)	Ameriško ministrstvo za energijo (DOE)	Pomoč organizacijam pri ocenjevanju in izboljševanju njihovih programov za kibernetsko varnost ter krepitvi njihove operativne odpornosti	Organizacije vseh sektorjev, vrst in velikosti	4	10 glavnih področij	metodologija in nabor orodij za samoocenjevanje	preglednica rezultatov s tortnimi grafikoni
Okvir za izboljšanje kibernetske varnosti kritične infrastrukture	Nacionalni inštitut za standarde in tehnologijo (NIST)	Okvir, namenjen usmerjanju dejavnosti na področju kibernetske varnosti in obvladovanju tveganj v organizacijah	Organizacije	N. R. (4 stopnje)	5 osrednjih funkcij	samoocenjevanje	-
Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2)	Pravna fakulteta Univerze v Katarju	Zagotoviti delujoči model, ki ga je mogoče uporabiti za primerjavo, merjenje in razvoj katarskega okvira za kibernetsko varnost	Katarske organizacije	5	5 glavnih področij	-	-
Certificiranje zrelosti na področju kibernetske varnosti (CMMC)	Ameriško ministrstvo za obrambo (DOD)	Spodbujanje najboljših praks na področju kibernetske varnosti za varovanje informacij	Organizacije sektorja obrambne industrijske baze (DIB)	5	17 glavnih področij	ocena s strani neodvisnih revizorjev	-
Zrelostni model kibernetske varnosti skupnosti (CCSMM)	Center za zagotavljanje in varnost infrastrukture (Centre for Infrastructure Assurance and Security) Univerze v Teksasu	Določi trenutno stanje skupnosti v zvezi z njeno pripravljenostjo na področju kibernetske varnosti in zagotoviti časovni načrt, ki mu bodo skupnosti sledile pri svojih prizadevanjih za pripravo	Skupnosti (lokalne ali državne uprave)	5	6 glavnih razsežnosti	ocenjevanje v skupnostih ob sodelovanju državnih in zveznih organov kazenskega pregona	-
Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (ISMM)	Visoka šola za računalništvo in inženiring (College of Computer Sciences and Engineering) Univerza King Fahd University of Petroleum and, Minerals, Dhahran, Savdska Arabija	Omogočanje organizacijam, da merijo svoj napredek pri izvajanju v daljšem časovnem obdobju in tako zagotovijo, da ohranjajo želeni položaj glede tveganja	Organizacije	5	23 ocenjenih področij	-	-
Model službe za notranjo revizijo za javni sektor (IA-CM)	Raziskovalna fundacija Inštituta notranjih revizorjev (Institute of Internal auditors Research Foundation)	Vzpostavitev zmogljivosti in zagovorništva na področju notranje revizije s pomočjo samoocenjevanja v javnem sektorju	Organizacije javnega sektorja	5	6 elementov	samoocenjevanje	-

Svetovni indeks kibernetske varnosti (GCI)	Mednarodna telekomunikacijska zveza (ITU)	Pregled zavez in razmer na področju kibernetske varnosti ter pomoč državam pri opredelitvi področij, na katerih so potrebne izboljšave na področju kibernetske varnosti	Države	n. r.	5 stebrov	samoocenjevanje	tabela z razvrstitvijo
Indeks kibernetske moči (CPI)	The Economist Intelligence Unit & Booz Allen Hamilton	Primerjati sposobnost držav skupine G20 v obrambi pred kibernetskimi napadi in pri uvajanju potrebne digitalne infrastrukture za uspešno in varno gospodarstvo.	Države skupine G20	n. r.	4 kategorije	primerjalna analiza, ki jo opravi podjetje Economist Intelligence Unit	tabela z razvrstitvijo

Preglednica 6 Primerjava ravni zrelosti

Model	Raven 1:	Raven 2:	Raven 3	Raven 4	Raven 5
Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM)	**Faza zagona** Zrelost na področju kibernetske varnosti ne obstaja ali pa je še v nerazviti fazi. Morda potekajo začetne razprave o krepitvi zmogljivosti na področju kibernetske varnosti, vendar konkretni ukrepi niso bili sprejeti. Na tej stopnji ni dokazov, ki bi jih bilo mogoče opazovati.	**Faza oblikovanja** Nekateri vidiki so se začeli širiti in oblikovati, vendar so lahko ad hoc narave, neorganizirani, slabo opredeljeni – ali preprosto „novi“. Vendar je mogoče dokaze o tej dejavnosti jasno prikazati	**Faza vzpostavitve** Elementi tega vidika so vzpostavljeni in delujejo. Vendar pa s tem povezana razporeditev sredstev ni dobro premišljena. V zvezi s „povezanimi“ naložbami v različne elemente tega vidika je bilo sprejetih malo kompromisov pri sprejemanju določitev. Vendar je ta vidik funkcionalen in opredeljen.	**Strateška faza** Sprejete so bile odločitve o tem, kateri deli tega vidika so pomembni in kateri so manj pomembni za posamezno organizacijo ali državo. Strateška faza odraža dejstvo, da so bile te odločitve sprejete glede na okoliščine države ali organizacije.	**Dinamična faza** Vzpostavljeni so jasni mehanizmi za spreminjanje strategije glede na prevladujoče okoliščine, kot so tehnologija v okolju grozenj, svetovni konflikti ali pomembne spremembe na enem zadevnem področju (npr. kibernetska kriminaliteta ali zasebnost). Dinamične organizacije so razvile metode za sprotno spreminjanje strategij. Na tej stopnji so značilni hitro odločanje, prerazporejanje virov in stalna pozornost na spreminjajoče se razmere.
Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2)	**MIL0 (RAVEN 0)** Prakse se ne izvajajo.	**MIL1 (RAVEN 1)** Začetne prakse se izvajajo, vendar so lahko ad hoc narave.	**MIL2 (RAVEN 2)** Značilnosti upravljanja: prakse so dokumentirane; za podporo procesu so na voljo ustrezna sredstva; osebje, ki izvaja prakse, ima ustrezne spretnosti in znanje; dodelijo se odgovornosti in pooblastila za izvajanje praks. Značilnost pristopa: Prakse so bolj popolne ali naprednejše kot pri MIL1.	**MIL3 (RAVEN 3)** Značilnosti upravljanja: dejavnosti so usmerjane s strani politik (ali drugih organizacijskih direktiv); cilji uspešnosti za dejavnosti na področju se določijo in spremljajo, da bi sledili dosežkom; dokumentirane prakse za dejavnosti na področju so standardizirane in izboljšane v celotnem podjetju. Značilnost pristopa: Prakse so bolj popolne ali naprednejše kot pri MIL2.	-

Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (ISMM)	Izvedeni postopek	Upravljani postopek	Vzpostavljen postopek	Predvidljiv postopek	Postopek optimizacije
Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2)	**Začetek:** na nekaterih področjih uporablja ad hoc prakse in postopke na področju kibernetske varnosti.	**Razvoj:** izvajajo se politike in prakse za razvoj in izboljšanje dejavnosti na področju kibernetske varnosti v okviru posameznih področij, da bi predlagali nove dejavnosti, ki jih je treba izvajati.	**Izvajanje:** sprejete so politike za izvajanje vseh dejavnosti na področju kibernetske varnosti v okviru posameznih področij s ciljem, da bi se izvajanje v določenem trenutku zaključilo.	**Prilagodljivost:** ponovno pregledovanje in revizija dejavnosti na področju kibernetske varnosti ter sprejem praks na podlagi napovednih kazalnikov, ki izhajajo iz preteklih izkušenj in ukrepov.	**Agilnost:** faza prilagajanja se še nadalje izvaja z dodatnim poudarkom na agilnosti in hitrosti pri izvajanju dejavnosti na posameznih področjih.
Certificiranje zrelosti na področju kibernetske varnosti (CMMC)	**Procesi: Izvedeni** Ker lahko organizacija te prakse izvaja le priložnostno in se zanaša ali se ne more zanašati na zrelost postopka dokumentiranja, se za raven 1 zrelost postopka ne ocenjuje. **Prakse: Osnovna kibernetska higiena** Raven 1 se osredotoča na zaščito zveznih informacij o pogodbah (FCI) in zajema le prakse, ki ustrezajo osnovnim zahtevam zaščite.	**Procesi: Dokumentirani** Raven 2 zahteva, da organizacija vzpostavi in dokumentira prakse in politike za usmerjanje izvajanja svojih prizadevanj v okviru modela CMMC. Dokumentacija o praksah posameznikom omogoča, da jih izvajajo na ponovljiv način. Organizacije razvijejo zrele zmogljivosti s pomočjo dokumentiranja svojih postopkov in nato z njihovim izvajanjem na način, kot je dokumentirano. **Prakse: Srednja kibernetska higiena** Raven 2 služi kot srednja raven med ravnjo 1 in ravnjo 3 in je sestavljena iz podskupine varnostnih zahtev, ki so določene v standardu NIST SP 800-171, ter praks iz drugih standardov in referenc.	**Procesi: Upravljani** Raven 3 zahteva, da organizacija pripravi, vzdržuje in financira načrt, ki prikazuje upravljanje dejavnosti za izvajanje praks. Načrt lahko vključuje informacije o poslanstvu, ciljih, projektnih načrtih, virih, potrebnem usposabljanju in sodelovanju ustreznih deležnikov. **Prakse: Dobra kibernetska higiena** Raven 3 se osredotoča na zaščito nadzorovanih nerazvrščenih informacij (CUI) in zajema vse varnostne zahteve, določene v standardu NIST SP 800-171, ter dodatne prakse iz drugih standardov in referenc za ublažitev nevarnosti.	**Procesi: Pregledani** Raven 4 zahteva, da organizacija pregleduje in meri učinkovitost praks. Poleg merjenja učinkovitosti praks lahko organizacije na tej ravni po potrebi sprejmejo korektivne ukrepe in redno obveščajo višje ravni upravljanja o stanju ali težavah. **Prakse: Proaktivne** Raven 4 se osredotoča na zaščito nadzorovanih nerazvrščenih informacij (CUI) in zajema podskupino okrepljenih varnostnih zahtev. Te prakse krepijo zmogljivosti organizacije za odkrivanje in odzivanje na spreminjajoče se taktike, tehnike in postopke ter prilagajanje nanje.	**Procesi: Optimizirani** Raven 5 zahteva, da organizacija standardizira in optimizira izvajanje postopkov v organizaciji. **Prakse: Napredne/proaktivne** Raven 5 se osredotoča na varovanje nadzorovanih nerazvrščenih informacij (CUI). Dodatne prakse povečujejo globino in izpopolnjenost zmogljivosti na področju kibernetske varnosti.
Zrelostni model kibernetske varnosti skupnosti (CCSMM)	**Ozaveščenost glede varnosti** Najpomembnejša dejavnost na tej ravni je ozaveščanje posameznikov in organizacij o grožnjah, težavah in vprašanjih, ki so povezana s kibernetsko varnostjo.	**Razvoj procesa** Raven je oblikovana za pomoč skupnostim pri vzpostavljanju in izboljševanju varnostnih postopkov, ki so potrebni za učinkovito obravnavo vprašanj na področju kibernetske varnosti.	**Omogočena informiranost** Namen je izboljšati mehanizme za izmenjavo informacij znotraj skupnosti, da bi lahko skupnost učinkovito povezala na videz različne informacije.	**Razvoj taktike** Elementi na tej ravni so zasnovani za razvoj boljših in bolj proaktivnih metod za odkrivanje napadov in odzivanje nanje. Na tej ravni bi morala biti vzpostavljena večina metod za preprečevanje.	**Polna varnostna operativna zmogljivost** Ta raven predstavlja tiste elemente, ki bi morali biti vzpostavljeni, če želi neka organizacija biti v celoti operativno pripravljena na spopadanje s katero koli vrsto kibernetske grožnje.

Model službe za notranjo revizijo za javni sektor (IA-CM)	**Začetna** Ni trajnostnih, ponovljivih zmogljivosti – odvisno od individualnih prizadevanj	**Infrastrukturna** Trajnostne in ponovljive prakse in postopki	**Integrirana** Enotno izvajanje upravljanja in poklicnih praks	**Upravljani** Vključuje informacije iz celotne organizacije za izboljšanje upravljanja in obvladovanja tveganj	**Optimizirani** Učenje s pomočjo informacij iz organizacije in zunaj nje za nenehno izboljševanje

Preglednica 7: Primerjava lastnosti/razsežnosti

	Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM)	Zrelostni model za zmogljivosti na področju kibernetske varnosti (C2M2)	Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti (Q-C2M2)	Certificiranje zrelosti na področju kibernetske varnosti (CMMC)	Certificiranje zrelosti na področju kibernetske varnosti (CMMC)	Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST (ISMM)	Okvir za izboljšanje kibernetske varnosti kritične infrastrukture	Svetovni indeks kibernetske varnosti (GCI)	Indeks kibernetske moči (CPI)
Ravni	Pet razsežnosti, razdeljenih na več dejavnikov, ki vključujejo več vidikov in kazalnikov (Slika 4)	Deset področij, vključno z edinstvenim ciljem upravljanja in več cilji pristopa (Slika 6)	Pet področij, razdeljenih na podpodročja	Sedemnajst področij, ki so razdeljena v procese, ter ena ali več zmogljivosti, ki so nato podrobno opisane v praksah (Slika 9).	Šest glavnih razsežnosti	Triindvajset ocenjenih področij	Pet funkcij z osnovnimi ključnimi kategorijami in podkategorijami (Slika 8).	Pet stebrov, ki vključuje več kazalnikov	Štiri kategorije z več kazalniki
Atributi/razsežnosti	i oblikovanje politike in strategije za kibernetsko varnost; ii spodbujanje odgovorne kulture na področju kibernetske varnosti v družbi; iii razvoj znanja o kibernetski varnosti; iv oblikovanje učinkovitih pravnih in regulativnih okvirov; v nadzor tveganj s pomočjo standardov, organizacij in tehnologij.	i Obvladovanje tveganja ii upravljanje sredstev, sprememb in konfiguracij; iii upravljanje identitete in dostopa; iv obvladovanje groženj in ranljivosti; v zavedanje o razmerah vi odziv na dogodke in incidente; vii upravljanje dobavne verige in zunanje odvisnosti; viii upravljanje delovne sile; ix arhitektura kibernetske varnosti; x upravljanje programa za kibernetsko varnost.	i Razumevanje (kibernetsko upravljanje, sredstva, tveganja in usposabljanje); ii Varnost (varnost podatkov, varnost tehnologije, nadzor dostopa, varnost komunikacij in varnost osebja); iii Izpostavljenost (spremljanje, obvladovanje incidentov, odkrivanje, analiza in izpostavljenost); iv Odzivanje (načrtovanje odzivov, blažitev in odziv); v Vzdrževanje (načrtovanje sanacije, upravljanje neprekinjenega poslovanja, izboljšanje in zunanja odvisnost).	i Nadzor dostopa ii Upravljanje sredstev iii Revizija in odgovornost iv Ozaveščenost in usposabljanje v Upravljanje konfiguracij vi Identifikacija in avtentikacija vii Odzivanje na incidente viii Vzdrževanje ix Zaščita medijev x Varnost osebja xi Fizično varovanje xii Sanacija (obnovitev) xiii Obvladovanje tveganja xiv Ocena varnosti xv zavedanje o razmerah xvi Zaščita sistemov in komunikacij xvii Celovitost sistema in informacij	i obravnavanje groženj, ii metrike, iii izmenjava informacij, iv tehnologija, v usposabljanje, vi preizkus.	i Upravljanje sredstev ii poslovno okolje, iii upravljanje, iv ocena tveganja, v strategija obvladovanja tveganj, vi ocena skladnosti, vii Nadzor dostopa viii Ozaveščenost in usposabljanje ix varnost podatkov, x procesi in postopki za varstvo podatkov, xi Vzdrževanje xii zaščitna tehnologija; xiii anomalije in dogodki, xiv stalno spremljanje varnosti, xv postopki odkrivanja, xvi načrtovanje odziva, xvii obveščanje o odzivu, xviii analiza odziva, xix blažitev odziva, xx izboljšanje odziva, xxi načrtovanje sanacije, xxii Izboljšanje izkoristka; xxiii obveščanje o sanaciji.	i Opredelitev ii Zaščita iii Odkrivanje iv Odzivanje v Obnovitev	i Pravni; ii Tehnični; iii Organizacijski; iv Izgradnja zmogljivosti; v Sodelovanje.	i Pravni in regulativni okvir ii Gospodarsko in socialno ozadje iii Tehnološka infrastruktura iv Uporaba v industriji

PRILOGA B – BIBLIOGRAFIJA TEORETIČNE RAZISKAVE

Almuhammadi, S. in Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework (Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST)“, v Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. in Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework (Zrelostni model informacijske varnosti za okvir kibernetske varnosti NIST)“, v Computer Science & Information Technology (CS & IT). Na voljo na: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs (Ocena stanja, analiza in priporočila o zaščiti kritične informacijske infrastrukture). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application (Razvoj modelov zrelosti za upravljanje informacijske tehnologije – model postopka in njegova uporaba). Na voljo na: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgijska vlada (2012): Strategija za kibernetsko varnost. Na voljo 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. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide (Razvoj zmogljivosti kibernetske varnosti: Priročnik o potrditvi koncepta). RAND Corporation. Na voljo 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 v donosnost naložb v varnost).

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019), Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (Zrelostni model za zmogljivosti na področju kibernetske varnosti, različica 2.0). Na voljo na https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center za varnostne študije (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland (Primerjava nacionalnih strategij za kibernetsko varnost – izzivi za Švico). Na voljo 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

Council of Ministers (2019), Portugalski uradni list, serija 1 – št. 108 - Resolution of the Council of Ministers No. 92/2019. Na voljo na: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016), Cybersecurity Capacity Maturity Model for Nations (CMM). Univerza v Oxfordu.

Cybercrime@IPA Projekt Sveta Evrope in Evropske unije, Globalni projekt za kibernetski kriminal Sveta Evrope in projektne skupine Evropske unije za kibernetski kriminal (2011), Specializirane enote za kibernetski kriminal – Študija dobre prakse. Na voljo na: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Danska vlada – ministrstvo za finance (2018), Danska strategija za kibernetsko varnost in varnost informacij. Na voljo na: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

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

Darra, E. (ni datuma) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting (Tehnične smernice za poročanje o incidentih.). Na voljo 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 (Tehnične smernice o varnostnih ukrepih). Na voljo 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 (Smernice o grožnjah in sredstvih). Na voljo na: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016): Cybersecurity Strategy (Strategija za kibernetsko varnost). Na voljo 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. *et al.* (2014): *Privacy and data protection by design - from policy to engineering* (Vgrajena zasebnost in vgrajeno varstvo podatkov – od politike do inženirstva). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Evropska agencija za varnost omrežij in informacij (2012), NCSS: Practical Guide on Development and Execution (Nacionalna strategija za kibernetsko varnost: Praktični vodnik za razvoj in izvajanje). Heraklion: ENISA.

Evropska agencija za varnost omrežij in informacij (2012), NCSS: Setting the course for national efforts to strengthen security in cyberspace (Nacionalna strategija za kibernetsko varnost: Določitev poti za nacionalna prizadevanja za okrepitev varnosti v kibernetskem prostoru). Heraklion: ENISA.

Evropska agencija za varnost omrežij in informacij (2016), Guidelines for SMEs on the security of personal data processing (Smernice za MSP o varnosti obdelave osebnih podatkov).

Evropska agencija za varnost omrežij in informacij (2016), NCSS good practice guide: designing and implementing national cyber security strategies (Vodič po dobrih praksah nacionalnih strategij za kibernetsko varnost: oblikovanje in izvajanje nacionalnih strategij za kibernetsko varnost). Heraklion: ENISA.

Evropska komisija (2012), Uredba Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu. Na voljo na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Evropska unija in Agencija za varnost omrežij in informacij (2014), *ENISA CERT inventory inventory of CERT teams and activities in Europe* (*ENISA, popis inventarja skupin CERT in dejavnosti v Evropi*. Na voljo na: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Evropska unija in Agencija za varnost omrežij in informacij (2017), Handbook on security of personal data processing (Priročnik o varnosti obdelave osebnih podatkov). Na voljo na: http://dx.publications.europa.eu/10.2824/569768

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies (Izvršni urad predsednika, Memorandum za vodje izvršnih oddelkov in agencij). Na voljo na: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Federal Chancellery of the Republic of Austria (2013) Austrian Cyber Security Strategy (Urad zveznega kanclerja Republike Avstrije, Avstrijska strategija za kibernetsko varnost). Na voljo 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

Federal Ministry of the Interior (2011) Cyber Security Strategy for Germany (Zvezno ministrstvo za notranje zadeve, Strategija za kibernetsko varnost za Nemčijo). Na voljo 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 o varnosti omrežij in informacij ter nacionalni standardi informacijske varnosti in zasebnosti za MSP: priporočila za izboljšanje sprejetja standardov varnosti informacij in zasebnosti v malih in srednjih podjetjih). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Evropska unija in Evropska agencija za varnost omrežij in informacij, (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations (Poročilo za leto 2015 o nacionalnih in mednarodnih vajah na področju kibernetske varnosti: anketa, analiza in priporočila). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Galan Manso, C. idr. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises (Standardi informacijske varnosti in zasebnosti za MSP: priporočila za izboljšanje sprejetja standardov varnosti informacij in zasebnosti v malih in srednjih podjetjih). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) „Evaluating Business Process Maturity Models (Ocena modelov zrelosti poslovnih procesov)“, Journal of the Association for Information Systems. Na voljo na: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Grška vlada (2017), Nacionalna strategija za kibernetsko varnost. Na voljo 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

Hrvaška vlada (2015), Nacionalna strategija Republike Hrvaške za kibernetsko varnost. Na voljo na: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Institute of Internal Auditors (ur.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide (Model službe za notranjo revizijo za javni sektor (IA-CM): pregled in priročnik za uporabo). Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Irska vlada (2019), Nacionalna strategija za kibernetsko varnost. Na voljo na: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

J.D., R. D. B. (2019) „Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework (Katarski zrelostni model za zmogljivosti na področju kibernetske varnosti in zakonodajni okvir)“, International Review of Law.

Latvijska vlada (2014), Cyber Security Strategy of Latvia (Strategija Latvije za kibernetsko varnost). Na voljo na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014): An evaluation framework for national cyber security strategies (Ocenjevalni okvir za nacionalne strategije za kibernetsko varnost). Heraklion: ENISA. Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Madžarska vlada (2018), Strategy for the Security of Network and Information Systems (Strategija za varnost omrežij in informacijskih sistemov). Na voljo 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

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks (Metodologije za prepoznavanje sredstev in storitev kritične informacijske infrastrukture: smernice za kartiranje elektronskih komunikacijskih omrežij).* Na voljo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Mednarodna telekomunikacijska zveza (ITU) (2018), Guide to developing a national cybersecurity strategy (Vodnik za razvoj nacionalne strategije za kibernetsko varnost). Na voljo na: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Mednarodna telekomunikacijska zveza (ITU) (2018), The Global Cybersecurity Index (Svetovni indeks kibernetske varnosti). Na voljo na: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Ministry for Competitiveness and Digital, Maritime and Services Economy (Ministrstvo za konkurenčnost ter digitalno, pomorsko in storitveno gospodarstvo) (2016), Malta Cyber Security Strategy (Strategija Malte za kibernetsko varnost). Na voljo 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

Ministry of Economic Affairs and Communications (2019) Cybersecurity Strategy – Republic of Estonia (Ministrstvo za gospodarske zadeve in komunikacije: Strategija za kibernetsko varnost – Republika Estonija). Na voljo na: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministry of National Defence Republic of Lithuania (2018) National Cyber Security Strategy (Ministrstvo za nacionalno obrambo Republike Litve: Nacionalna strategija za kibernetsko varnost).

Nacionalne strategije za kibernetsko varnost – interaktivni zemljevid (ni datuma). Na voljo na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Nacionalni inštitut za standarde in tehnologijo (2018), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (Okvir za izboljšanje kibernetske varnosti kritične infrastrukture, različica 1.1) Gaithersburg, MD: National Institute of Standards and Technology. Na voljo na: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Cyber Security Centre (2015) National Cyber Security Strategy of the Czech Republic (Nacionalni center za kibernetsko varnost: Nacionalna strategija Češke republike za kibernetsko varnost). Na voljo na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cybersecurity Strategies Evaluation Tool (Orodje za ocenjevanje nacionalnih strategij za kibernetsko varnost) (2018). Na voljo na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Object Management Group (2008) Business Process Maturity Model (Model za zorenje poslovnih procesov). Na voljo na: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Evropska unija in Skupno raziskovalno središče – Evropska komisija (2008), Handbook on Constructing Composite Indicators: Methodology and User Guide (Priročnik za izdelavo sestavljenih kazalnikov: metodologija in uporabniški priročnik). OECD. Na voljo na: https://www.oecd.org/sdd/42495745.pdf.

Office of the commissioner of Electronic Communications and Postal Regulations (2012) Cybersecurity Strategy of the Republic of Cyprus (Strategija Republike Ciper za kibernetsko varnost).

Organizacija za gospodarsko sodelovanje in razvoj (Organisation for Economic Co-operation and Development) (OECD) (2012) Cybersecurity policy making at a turning point (Oblikovanje politike kibernetske varnosti na prelomni točki). Na voljo na: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) Good Practice Guide on National Exercises (Vodnik dobrih praks za nacionalne vaje).

Ouzounis, E. (2012), National Cyber Security Strategies - Practical Guide on Development and Execution (Nacionalne strategije za kibernetsko varnost - praktični vodnik za razvoj in izvajanje).

Poročilo o kibernetskih incidentih in analitični sistem – orodje za vizualno analizo (ni datuma). Na voljo na: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Portesi, S. (2017) Izboljšanje sodelovanja med skupinami CSIRT in organi kazenskega pregona: Pravni in organizacijski vidiki

Predsedstvo Sveta ministrov (2017) - Italijanski akcijski načrt za kibernetsko varnost. Na voljo 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. Na voljo na: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Romunska vlada (2013), Strategija Romunije za kibernetsko varnost. Na voljo 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. in European Union Agency for Cybersecurity (Agencija Evropske unije za kibernetsko varnost) (2019), Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies (Dobre prakse na področju inovacij v kibernetski varnosti v okviru nacionalne strategije za kibernetsko varnost). Na voljo na: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariat of the Security Committee (2019) Finland's Cyber Security Strategy 2019 (Finska strategija za kibernetsko varnost 2019). Na voljo na: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovaška vlada (2015), Cyber Security Concept of the Slovak Republic (Koncept kibernetske varnosti Slovaške republike). Na voljo 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) Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 (Direktiva 2010/41/EU Evropskega parlamenta in Sveta z dne 7. julija 2010).

Smith, R. (2016) „Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 (Direktiva 2010/41/EU Evropskega parlamenta in Sveta z dne 7. julija 2010)", v Smith, R., Core EU Legislation. London: Macmillan Education. Na voljo na: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32010L0041.

Stavropoulos, V. (2017), European Cyber Security Month 2017 (Evropski mesec kibernetske varnosti 2017).

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

The Federal Council (2018) National strategy for the protection of Switzerland against cyber risks (Nacionalna strategija za zaščito Švice pred kibernetskimi tveganji).

The Luxembourguish Government Council (2018) National Cybersecurity Strategy (Luksemburški vladni svet: Nacionalna strategija za kibernetsko varnost). Na voljo 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

The Netherlands Governement (2018), National Cyber Security Agenda (Nizozemska vlada: Nacionalna agenda za kibernetsko varnost). Na voljo 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

The White House (2018) National Cyber Strategy of the United States of America (Bela hiša: Nacionalna kibernetska strategija Združenih držav Amerike). Na voljo na: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

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

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report (Ocene tveganja na nacionalni ravni: analitično poročilo).* Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management (Poročilo o sodelovanju in upravljanju na področju kibernetskih kriz). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises (Poročilo o sodelovanju in upravljanju na področju kibernetskih kriz: skupne prakse kriznega upravljanja na ravni EU in uporabnost za področje kibernetskih kriz). Na voljo na: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021 (2016) (Nacionalna strategija Združenega kraljestva za kibernetsko varnost 2016–2021). Na voljo na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck et al. (2009): Understanding Maturity Models (Razumevanje modelov zrelosti).

Urad francoskega predsednika vlade (2014), Francoska nacionalna strategija za digitalno varnost. Na voljo na: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Uradni list Evropske unije (2008) DIREKTIVA SVETA 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite. Na voljo na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Vlada Bolgarije (2015), National Cyber Security Strategy - Cyber-resistant Bulgaria 2020 (Nacionalna strategija za kibernetsko varnost – Bolgarija 2020, odporna proti kibernetski varnosti).

Vlada Španije (2019), Nacionalna strategija za kibernetsko varnost. Na voljo 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

Wamala, D. F. (2011), „ITU National Cybersecurity Strategy Guide“ (Navodila ITU za nacionalno strategijo za kibernetsko varnost). Na voljo na: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) „The Community Cyber Security Maturity Model“ (Zrelostni model kibernetske varnosti skupnosti), v 2007, 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

Zrelost CSIRT – orodje za samoocenjevanje (brez datuma). Na voljo na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

PRILOGA C – DRUGI PREUČENI CILJI

V okviru faze teoretičnega raziskovanja in razgovorov, ki jih je opravila agencija ENISA, so bili preučeni spodaj navedeni cilji. Naslednji cilji niso del okvira za ocenjevanje nacionalnih zmogljivosti, vendar osvetljujejo teme, o katerih je vredno razpravljati. Vsako od naslednjih podpoglavij bo pojasnilo, zakaj je bil cilj opuščen.

- Razvoj strategij kibernetske varnosti za posamezne sektorje
- Boj proti dezinformacijskim kampanjam
- varne najsodobnejše tehnologije (5G, umetna inteligenca, kvantno računalništvo ...);
- zagotavljanje podatkovne suverenosti in
- zagotavljanje spodbud za razvoj industrije kibernetskega zavarovanja.

Razvoj strategij kibernetske varnosti za posamezne sektorje

Sprejetje sektorskih strategij, ki so namenjene sektorskim intervencijam in spodbudam, zagotovo uvaja močnejšo decentralizirano zmogljivost. Zlasti je primerno za države članice, katerih izvajalci bistvenih storitev se morajo ukvarjati z različnimi okviri in predpisi ter v katerih je zaradi transverzalne narave kibernetske varnosti veliko odvisnosti. V več državah članicah je skupno, da imajo veliko nacionalnih in regulatornih organov, ki poznajo posebnosti vsakega sektorja in imajo mandat za izvrševanje posebnih predpisov za vsak sektor.

Danska je na primer začela izvajati šest ciljno usmerjenih strategij, ki obravnavajo prizadevanja najbolj kritičnih sektorjev za kibernetsko varnost in varnost informacij, da bi razvila močnejšo decentralizirano zmogljivost na področju kibernetske varnosti in varnosti informacij. Vsaka „sektorska enota“ bo med drugim prispevala k ocenam ogroženosti na sektorski ravni, spremljanju, vajah pripravljenosti, vzpostavitvi varnostnih sistemov, izmenjavi znanja in navodilom. Sektorske strategije zajemajo naslednje sektorje:

- energija,
- zdravstvo,
- promet,
- telekomunikacije,
- finance in
- pomorski promet.

Druge države članice so izrazile interes za razmislek o sektorskih strategijah za kibernetsko varnost, ki bi odražale vse regulativne zahteve. Vendar je treba opozoriti, da tak cilj morda ne bo ustrezal vsem državam članicam, kar je odvisno od njihove velikosti, nacionalnih politik in zrelosti. Agencija ENISA zaradi velikih težav pri zagotavljanju, da bi okvir upošteval vse specifičnosti, tega cilja ni vključila v okvir.

Boj proti dezinformacijskim kampanjam

Države članice v svoje nacionalne strategije za kibernetsko varnost vključujejo varstvo temeljnih načel, kot so človekove pravice, preglednost in zaupanje javnosti. To je zelo pomembno zlasti v zvezi z dezinformacijami, ki se razširjajo prek tradicionalnih informativnih medijev ali družbenih medijev. Poleg tega je kibernetska varnost trenutno eden največjih izzivov v okviru volitev. V času pred pomembnimi volitvami so bile v različnih državah dejansko opažene dejavnosti, kot

sta širjenje lažnih informacij ali negativna propaganda. Ta grožnja lahko ogrozi demokratični proces EU. Na evropski ravni je Komisija predstavila akcijski načrt[32] za okrepitev prizadevanj za boj proti dezinformacijam v Evropi: ta načrt se osredotoča na 4 ključna področja (odkrivanje, sodelovanje, sodelovanje s spletnimi platformami in ozaveščenost) ter je namenjen krepitvi zmogljivosti EU in sodelovanja med državami članicami.

Štiri od 19 držav, s katerimi so bili opravljeni pogovori, so izrazile namero, da bodo v svoji nacionalni strategiji za kibernetsko varnost obravnavale dezinformacije in propagando.

Francoska nacionalna strategija za kibernetsko varnost[33] na primer ugotavlja, da: „je država odgovorna za obveščanje državljanov o tveganjih na področju manipulacij in propagandnih tehnik, ki jih uporabljajo zlonamerni akterji na internetu. Po terorističnih napadih na Francijo januarja 2015 je vlada na primer vzpostavila informacijsko platformo o tveganjih, povezanih z islamsko radikalizacijo prek elektronskih komunikacijskih omrežij: « Stop-djihadisme.gouv.fr ».“ Ta pristop bi lahko razširili in uporabili pri odzivu na druge pojave propagande ali destabilizacije.

V drugem primeru je v poljski nacionalni strategiji za kibernetsko varnost za obdobje 2019–2024[34] navedeno, da: „pri manipulativnih dejavnostih, kot so dezinformacijske kampanje, so potrebni sistemski ukrepi za ozaveščanje državljanov v povezavi s preverjanjem avtentičnosti informacij in odzivanjem na poskuse njihovega izkrivljanja.“

Vendar se je več držav članic med razgovori, ki jih je opravila agencija ENISA, strinjalo, da tega vprašanja ne obravnavajo v okviru svojih nacionalnih strategij za kibernetsko varnost kot grožnjo kibernetski varnosti, temveč obravnavajo to vprašanje na širši družbeni ravni, na primer prek pobud politike.

Varne najnovejše tehnologije (5G, umetna inteligenca, kvantno računalništvo ...)

Glede na to, da se sedanje okolje kibernetskih groženj še naprej širi, bo razvoj novih tehnologij najverjetneje povzročil povečanje intenzivnosti in števila kibernetskih napadov ter diverzifikacijo metod, sredstev in ciljev, ki jih uporabljajo akterji groženj. Medtem lahko te nove tehnološke rešitve v obliki najsodobnejših tehnologij postanejo gradniki evropskega digitalnega trga. Za zaščito vse večje digitalne odvisnosti držav članic in zaradi pojava novih tehnologij bi bilo treba oblikovati spodbude in celovite politike, ki bi bile v podporo varnemu in zanesljivemu razvoju in uporabi teh tehnologij v EU.

V fazi teoretične raziskave, ki je vključevala pregled nacionalnih strategij za kibernetsko varnost držav članic, so bile kot zanimive za države članice predlagane naslednje najsodobnejše tehnologije: 5G, umetna inteligenca, kvantno računalništvo, kriptografija, računalništvo na robu, povezana in avtonomna vozila, vele- in pametni podatki, blokovna veriga, robotika in internet stvari.

Evropska komisija je v začetku leta 2020 objavila sporočilo, v katerem je države članice pozvala, naj sprejmejo ukrepe za izvajanje sklopa ukrepov, ki so bili priporočeni v sklepih o naboru orodij za 5G[35]. Ta nabor orodij za 5G je nastal na podlagi Priporočila (EU) 2019/534 o kibernetski varnosti omrežij 5G, ki ga je Komisija sprejela leta 2019 in v katerem je pozvala k enotnemu evropskemu pristopu k varnosti omrežij 5G[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/EN/TXT/?uri=CELEX%3A32019H0534

Med razgovori, ki jih je opravila agencija ENISA, je bilo poudarjeno, da je to bolj horizontalna tema, ki se obravnava v okviru nacionalne strategije za kibernetsko varnost in ne kot specifični cilj sam po sebi.

Zagotavljanje podatkovne suverenosti

Po eni strani je mogoče kibernetski prostor razumeti kot močan skupni svetovni prostor, ki je lahko dostopen, zagotavlja visoko stopnjo povezljivosti in lahko ponudi velike priložnosti za družbeno-gospodarsko rast. Po drugi strani pa so za kibernetski prostor značilni tudi njegova šibka pristojnost, težave pri pripisovanju dejanj, pomanjkanje meja in medsebojno povezani sistemi, ki so lahko porozni in katerih podatki so lahko ukradeni ali celo dostopni tujim vladam. Poleg teh dveh vidikov je digitalni ekosistem zaznamovan s koncentracijo spletnih platform in infrastrukture za storitve, ki je v rokah majhnega števila deležnikov. Vsi navedeni vidiki vodijo države članice k spodbujanju digitalne suverenosti. Doseganje digitalne suverenosti pomeni, da lahko državljani in podjetja v celoti poslujejo z uporabo digitalnih storitev in izdelkov IKT, ki so zanesljivi, in so lahko brez strahu v zvezi z osebnimi podatki ali digitalnimi sredstvi, ekonomsko avtonomijo ali političnim vplivom posameznika.

Države članice se zavzemajo za suverenost podatkov ali digitalno suverenost na nacionalni in evropski ravni. Čeprav se zdi, da države članice tega vprašanja ne obravnavajo neposredno v svojih nacionalnih strategijah za kibernetsko varnost kot specifični cilj, ga obravnavajo kot horizontalno načelo ali pa svojo namero, da zagotovijo digitalno suverenost na nacionalni ravni, orišejo v priložnostnih publikacijah s poudarkom na ključnih tehnologijah. V francoskem strateškem pregledu kibernetske obrambe iz leta 2018 je bilo na primer navedeno: „nadzor nad naslednjimi tehnologijami je bistvenega pomena za zagotovitev digitalne suverenosti: šifriranje komunikacije, zaznavanje kibernetskih napadov, zasebni mobilni radio, računalništvo v oblaku in umetna inteligenca“[37].

Na evropski ravni države članice dejavno sodelujejo pri opredelitvi evropske strategije za podatke (COM/2020/66 final) in oblikovanju certifikacijskega okvira EU za digitalne proizvode, storitve in postopke IKT, vzpostavljenega z Aktom EU o kibernetski varnosti (2019/881), da se zagotovi strateška digitalna avtonomija na evropski ravni.

Faza razgovorov z državami članicami je pokazala, da se vprašanje digitalne suverenosti pogosto obravnava kot širše vprašanje, ki ni omejeno le na področje kibernetske varnosti. Zato države članice te teme ne obravnavajo v svojih nacionalnih strategijah za kibernetsko varnost, maloštevilne države, ki pa temo vključujejo, pa je ne obravnavajo kot poseben cilj sam po sebi.

Zagotavljanje spodbud za razvoj industrije kibernetskega zavarovanja

Trenutno stanje v industriji kibernetskega zavarovanja kaže, da se je svetovni trg nedvomno povečal. Vendar je še vedno v začetni fazi, saj je treba še vedno zbirati podatke in določiti številne precedense (*npr.* tiha pokritost, sistemska kibernetska tveganja ...). Poleg tega so ocenjene izgube, ki izhajajo iz kibernetskih napadov po vsem svetu, za več redov večje od sedanjih zmogljivosti za kritje v sektorju kibernetskega zavarovanja (delovni dokument MDS – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143 (Kibernetsko tveganje za finančni sektor: okvir za kvantitativno oceno)). Vendar lahko razvoj industrije kibernetskega zavarovanja zagotovo prinese koristi in postavi temelje za učinkovite mehanizme. Mehanizmi kibernetskega zavarovanja lahko dejansko pomagajo pri:

- ozaveščanju o tveganjih za kibernetsko varnost v podjetjih;

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

- kvantitativni oceni izpostavljenosti kibernetskim tveganjem;
- izboljšanju obvladovanja tveganj na področju kibernetske varnosti;
- zagotavljanju podpore organizacijam, ki so žrtve kibernetskih napadov;
- kritju škode (materialne ali ne), povzročene s kibernetskim napadom.

Nekatere države članice so začele obravnavati to vprašanje. Na primer:

- Estonija je v svoji nacionalni strategiji za kibernetsko varnost sprejela pristop „počakajmo in bomo videli“: „Za zmanjšanje kibernetskih tveganj v zasebnem sektorju na splošno bosta analizirana povpraševanje in ponudba storitev kibernetskega zavarovanja v Estoniji, na tej podlagi pa bodo dogovorjena načela sodelovanja za povezane strani, vključno z izmenjavo informacij, pripravo ocene tveganja itd. Danes je malo ponudnikov storitev kibernetskega zavarovanja na estonskem trgu, zato je treba najprej ugotoviti, kdo kaj ponuja. Zapletenost glede zaščite zavarovanja se pogosto šteje za oviro za razvoj trga kibernetskega zavarovanja.“
- Luksemburg izrecno podpira razvoj industrije kibernetskega zavarovanja v svoji nacionalni strategiji za kibernetsko varnost: „Cilj 1: Ustvarjanje novih proizvodov in storitev. Da bi združili tveganja in spodbudili žrtve digitalnih kibernetskih incidentov, naj poiščejo pomoč strokovnjakov pri obvladovanju incidenta in obnovi sistema, ki ga je prizadelo zlonamerno dejanje, bodo zavarovalnice pozvane k oblikovanju posebnih produktov na področju kibernetskega zavarovanja.“

Povratne informacije v razgovorih so bili pri tej temi precej različne: nekatere države članice so izjavile, da je vprašanje kibernetskega zavarovanja nedavno postalo tema razprave, druge pa so se strinjale, da čeprav je tema obetavna, industrija še ni dovolj zrela. Vendar je veliko vprašanih izjavilo, da se ta tema ne obravnava kot del nacionalne strategije za kibernetsko varnost, ker se je štela za preveč specifično ali pa ni spadala v okvir nacionalne strategije za kibernetsko varnost.

TP-02-21-253-SL-N

O Agenciji Evropske unije za kibernetsko varnost

Agencija Evropske unije za kibernetsko varnost, ENISA, je agencija Unije, katere cilj je dosegati visoko skupno raven kibernetske varnosti po vsej Evropi. Ustanovljena je bila leta 2004, njene pristojnosti pa so bile okrepljene z uredbo EU o kibernetski varnosti. Prispeva h kibernetski politiki EU, povečuje zaupanje v produkte, storitve in procese IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi, da bo pripravljena na kibernetske izzive prihodnosti. Z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter na koncu zagotovila digitalno varnost evropske družbe in državljanov. Za več informacij obiščite spletno stran 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: 978-92-9204-494-7
DOI: 10.2824/380323