EUROPEAN UNION AGENCY
FOR CYBERSECURITY

VALSTS SPĒJU NOVĒRTĒŠANAS SISTĒMA

2020. GADA DECEMBRIS

PAR *ENISA*

Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir Savienības aģentūra, kuras mērķis ir panākt vienādi augsta līmeņa kiberdrošību visā Eiropā. Eiropas Savienības Kiberdrošības aģentūra, kas dibināta 2004. gadā un nostiprināta ar ES Kiberdrošības aktu, sniedz ieguldījumu ES kiberdrošības politikā, stiprina IKT produktu, pakalpojumu un procesu uzticamību ar kiberdrošības sertifikācijas shēmām, sadarbojas ar dalībvalstīm un ES struktūrām un palīdz Eiropai sagatavoties nākotnes izaicinājumiem kiberdrošības jomā. Daloties zināšanās, veidojot spējas un veicinot izpratni, Aģentūra sadarbojas ar savām galvenajām ieinteresētajām personām, lai vairotu uzticību savienotajai ekonomikai, palielinātu Savienības infrastruktūras noturību un visbeidzot garantētu Eiropas sabiedrībai un iedzīvotājiem digitālo drošību. Plašāku informāciju skatiet vietnē www.enisa.europa.eu.

KONTAKTINFORMĀCIJA

Ar autoriem var sazināties, rakstot uz team@enisa.europa.eu.
Plašsaziņas līdzekļu jautājumus par šo dokumentu lūdzam sūtīt uz press@enisa.europa.eu.

AUTORI

Anna Sarri, *Pinelopi Kyranoudi* — Eiropas Savienības Kiberdrošības aģentūra (*ENISA*)
Aude Thirriot, *Federico Charelli*, *Yang Dominique* — *Wavestone*

PATEICĪBAS

ENISA vēlas pateikties un paust atzinību visiem ekspertiem, kas piedalījās šā ziņojuma sagatavošanā un sniedza tajā vērtīgu ieguldījumu, jo īpaši šiem ekspertiem (alfabēta secībā):

Valsts centrālais digitālās sabiedrības attīstības birojs (Ungārija), *Marin Ante Pivcevic*,

Kiberdrošības centrs (Beļģija),

CFCS — Center for Cybersikkerhed (Dānija), *Thomas Wulff*,

Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *Alzofra Martinez Alvaro*,

Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *Adrian-Ionut Bobeica*,

Federālā iekšlietu ministrija (Vācija), *Sascha-Alexander Lettgen*,

Informācijas drošības pārvalde (Slovēnijas Republika), *Marjan Kavčič*,

Itālijas valdība (Itālija),

Maltas Informācijas tehnoloģiju aģentūra (Malta), *Katia Bonello* un *Martin Camilleri*,

Tieslietu un sabiedriskās drošības ministrija (Norvēģija), *Robin Bakke*,

Digitālās politikas ministrija (Grieķija), *George Drivas*, *Nestoras Chouliaras*, *Evgenia Tsaprali* un *Sotiris Vasilos*,

Ekonomikas un komunikācijas ministrija (Igaunija), *Anna-Liisa Pärnalaas*,

Valsts kiberdrošības un informācijas drošības aģentūra (Čehijas Republika), *Veronika Netolická*,

Valsts drošības iestāde (Slovākija),

Valsts drošības departaments (Spānija), *Maria Mar Lopez Gil*,

NCTV, Tieslietu un drošības ministrija (Nīderlande),

Portugāles Valsts kiberdrošības centrs (Portugāle), *Alexandre Leite* un *Pedro Matos*,

Kiberdrošības politikas nodaļa, Vides, klimata un komunikācijas departaments (Īrija), *James Caffrey*,

Oksfordas Universitāte, Globālais kiberdrošības spēju centrs, *Carolin Weisser Harris*.

ENISA vēlas pateikties par vērtīgo devumu šajā pētījumā arī visiem tiem ekspertiem, kas piedalījās, bet vēlējās palikt anonīmi.

JURIDISKS PAZIŅOJUMS

Jāņem vērā, ka šajā publikācijā ir sniegts *ENISA* viedoklis un interpretācija, ja vien nav norādīts citādi. Šī publikācija nav *ENISA* vai *ENISA* struktūru dokuments ar juridiskām sekām, ja vien tā netiek pieņemta saskaņā ar Regulu (ES) 2019/881.
Šajā publikācijā var nebūt atspoguļoti jaunākie tehnoloģiskie sasniegumi, un *ENISA* to var ik pa laikam atjaunināt.

Pēc vajadzības ir norādīti ārējie avoti. *ENISA* neatbild par šajā publikācijā minēto ārējo avotu, tostarp ārējo tīmekļa vietņu, saturu.

Šī publikācija ir tikai informatīva. Tai jābūt pieejamai bez maksas. Ne *ENISA*, ne personas, kas rīkojas tās vārdā, neatbild par to, kā tiek izmantota šajā publikācijā iekļautā informācija.

PAZIŅOJUMS PAR AUTORTIESĪBĀM

ISBN: 978-92-9204-443-5

DOI: 10.2824/590072

KATALOGS: TP-06-20-047-EN-N

1. SATURS

TERMINU VĀRDNĪCA

AKRONĪMS	DEFINĪCIJA
AI	Mākslīgais intelekts
C2M2	Kiberdrošības spēju gatavības modelis
CCRA	Vienošanās par kopējo kritēriju atzīšanu
CCSMM	Pašvaldību kiberdrošības gatavības modelis
IKI	Informācijas kritiskā infrastruktūra
CMM	Kiberdrošības spēju gatavības modelis valstīm
CMMC	Kiberdrošības gatavības modeļa sertifikācija
CPI	Kiberspēcīguma indekss
CSIRT	Datordrošības incidentu reaģēšanas vienība
CVD	Koordinēta ievainojamību atklāšana
DPA	Datu aizsardzības likums
DVT	Digitālais vienotais tirgus
ECCG	Eiropas Kiberdrošības sertifikācijas grupa
ECSM	Eiropas kiberdrošības mēnesis
ECSO	Eiropas Kiberdrošības organizācija
EBTA	Eiropas Brīvās tirdzniecības asociācija
EKI	Eiropas kvalifikāciju ietvarstruktūra
ES	Eiropas Savienība
GCI	Globālais kiberdrošības indekss
VDAR	Vispārīgā datu aizsardzības regula
VDP	Valdības digitālais pakalpojums
IA-CM	Iekšējās revīzijas spēju modelis publiskajam sektoram
IKT	Informācijas un komunikācijas tehnoloģijas
ISMM	Informācijas drošības gatavības modelis *NIST* kiberdrošības satvaram
ITU	Starptautiskā Telesakaru savienība
TI	Tiesībaizsardzības iestāde
DV	Dalībvalsts
VKS	Valsts kiberdrošības stratēģija

TID	Tīklu un informācijas drošība
NIST	Nacionālais Standartu un tehnoloģijas institūts
VSK	Valsts sadarbības koordinators
PS	Pamatpakalpojumu sniedzējs
OT	Operāciju tehnoloģija
PET	Privātuma aizsardzības tehnoloģija
PIMS	Privātās informācijas pārvaldības sistēma
PPP	Publiskā un privātā sektora partnerība
Q-C2M2	Kataras kiberdrošības spēju gatavības modelis
PI	Pētniecība un izstrāde
MVU	Mazie un vidējie uzņēmumi
SOG-IS MRA	Augstāko amatpersonu grupa informācijas sistēmu drošības savstarpējās atzīšanas nolīguma jautājumos

KOPSAVILKUMS

Tā kā pašreizējā kiberdraudu aina turpina paplašināties un palielinās kiberuzbrukumu intensitāte un skaits, ES dalībvalstīm uz to ir iedarbīgi jāreaģē, turpinot attīstīt un pielāgot savas valsts kiberdrošības stratēģijas (VKS). Kopš 2012. gada, kad *ENISA* publicēja pirmos pētījumus par VKS, ES dalībvalstis un EBTA valstis ir guvušas lielus panākumus savu stratēģiju izstrādē un īstenošanā.

Šajā ziņojumā ir sniegts pārskats par darbu, ko *ENISA* veikusi, lai izveidotu valsts spēju novērtēšanas sistēmu (VSNS).

Sistēmas mērķis ir dot dalībvalstīm iespēju pašām novērtēt savu gatavības līmeni, novērtējot savus VKS mērķus, un tādējādi palīdzēt tām uzlabot un veidot kiberdrošības spējas gan stratēģiskā, gan darbības līmenī.

Tā sniedz vienkāršu, reprezentatīvu pārskatu par dalībvalsts gatavību kiberdrošības jomā. VSNS ir rīks, kas dalībvalstīm:

- sniedz noderīgu informāciju, kura palīdz izstrādāt ilgtermiņa stratēģiju (piem., laba prakse, pamatnostādnes);
- palīdz atklāt, kādu elementu VKS vēl trūkst;
- palīdz turpināt veidot kiberdrošības spējas;
- palīdz nodrošināt pārskatatbildību par politisko rīcību;
- palīdz vairot plašas sabiedrības un starptautisko partneru uzticību;
- palīdz labāk uzrunāt auditoriju un veidot pārredzamas organizācijas tēlu sabiedrībā;
- palīdz paredzēt gaidāmās problēmas;
- palīdz apzināt gūtās mācības un paraugpraksi;
- sniedz priekšstatu par kiberdrošības spēju kopējo līmeni ES, lai atvieglotu diskusijas;
- palīdz izvērtēt valsts spējas kiberdrošības jomā.

Šīs sistēmas veidošanā savu atbalstu sniedza attiecīgās jomas *ENISA* eksperti un 19 dalībvalstu un EBTA valstu pārstāvji[1]. Šis ziņojums ir paredzēts politikas veidotājiem, ekspertiem un valsts amatpersonām, kas atbild par valsts kiberdrošības stratēģijas un plašāk arī par kiberdrošības spēju veidošanu, īstenošanu un izvērtēšanu vai ir iesaistīti šajos uzdevumos.

[1] Tika intervēti pārstāvji no šādām dalībvalstīm un EBTA valstīm: Beļģija, Čehija, Dānija, Grieķija, Horvātija, Igaunija, Itālija, Īrija, Lihtenšteina, Malta, Nīderlande, Norvēģija, Portugāle, Slovākija, Slovēnija, Spānija, Ungārija, Vācija, Zviedrija.

Valsts spēju novērtēšanas sistēma aptver 17 stratēģiskos mērķus, kas ir iedalīti četrās lielās grupās.

- 1. grupa: kiberdrošības pārvaldība un standarti
  1. Izstrādāt valsts ārkārtas rīcības plānu kiberdrošības jomā
  2. Noteikt pamata drošības pasākumus
  3. Nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem

- 2. grupa: spēju veidošana un izpratnes vairošana
  4. Organizēt kiberdrošības mācības
  5. Radīt spējas reaģēt uz incidentiem
  6. Vairot lietotāju izpratni
  7. Stiprināt apmācības un izglītības programmas
  8. Veicināt PI
  9. Dot privātajam sektoram stimulus ieguldīt drošības pasākumos
  10. Uzlabot piegādes ķēdes kiberdrošību

- 3. grupa: juridiskie un normatīvie jautājumi
  11. Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus
  12. Apkarot kibernoziedzību
  13. Izveidot mehānismus ziņošanai par incidentiem
  14. Pastiprināt privātuma un datu aizsardzību

- 4. grupa: sadarbība
  15. Izveidot publiskā un privātā sektora partnerību
  16. Institucionalizēt sadarbību starp publiskā sektora aģentūrām
  17. Iesaistīties starptautiskajā sadarbībā

1. IEVADS

Saskaņā ar 2016. gada jūlijā pieņemtās Tīklu un informācijas drošības (TID) direktīvas 1. un 7. pantu ES dalībvalstīm ir jāpieņem valsts stratēģija par tīklu un informācijas sistēmu drošību (dēvēta arī par valsts kiberdrošības stratēģiju (VKS)). Šajā kontekstā VKS ir jāsaprot kā satvars, kurā ir noteikti stratēģiskie principi, pamatnostādnes, stratēģiskie mērķi, prioritātes un atbilstīga politika un regulatīvie pasākumi. Paredzētais VKS mērķis ir sasniegt un uzturēt tīklu un sistēmu drošību augstā līmenī, lai dalībvalstis varētu mazināt iespējamos draudus. Papildus tam VKS var arī veicināt rūpniecības, ekonomikas un sociālo attīstību.

ES Kiberdrošības aktā ir noteikts, ka *ENISA* veicina paraugprakses izplatīšanu VKS formulēšanas un īstenošanas jomā, sniedzot dalībvalstīm atbalstu TID direktīvas ieviešanā un apkopojot vērtīgas atsauksmes par dalībvalstu pieredzi. Tāpēc *ENISA* ir izveidojusi vairākus rīkus, kas palīdzēs dalībvalstīm izstrādāt, īstenot un izvērtēt savas valsts kiberdrošības stratēģijas (VKS).

Savu pilnvaru ietvaros *ENISA* plāno izstrādāt valsts spēju pašnovērtēšanas sistēmu, ar kuru varētu novērtēt dažādo VKS gatavības līmeni. Šā ziņojuma mērķis ir iepazīstināt ar pētījumu, kas veikts saistībā ar pašnovērtēšanas sistēmas formulēšanu.

1.1 PĒTĪJUMA DARBĪBAS JOMA UN MĒRĶI

Šā pētījuma galvenais mērķis ir izveidot valsts spēju pašnovērtēšanas sistēmu (tālāk tekstā "VSNS"), ar ko novērtēt dalībvalstu kiberdrošības spēju gatavības līmeni. Konkrētāk, šai sistēmai vajadzētu palīdzēt valstīm:

- izvērtēt savas valsts kiberdrošības spējas;
- gūt labāku izpratni par valsts gatavības līmeni;
- noteikt jomas, kurās nepieciešami uzlabojumi;
- veidot kiberdrošības spējas.

Šai sistēmai būtu jāpalīdz dalībvalstīm, un jo īpaši valsts politikas veidotājiem, veikt pašnovērtējumu, lai varētu uzlabot valsts kiberdrošības spējas.

1.2 METODISKĀ PIEEJA

Valsts spēju pašnovērtēšanas sistēmas izstrādei izmantotā metodiskā pieeja sastāvēja no četriem posmiem.

1. **Dokumentu izpēte**. Pirmajā posmā tika veikta plaša publikāciju izpēte, lai apzinātu valsts kiberdrošības stratēģiju gatavības novērtēšanas sistēmu izstrādes paraugpraksi. Dokumentu izpētē galvenokārt tika sistemātiski analizēti attiecīgi dokumenti par kiberdrošības spēju veidošanu un stratēģijas noteikšanu, aplūkotas pastāvošās dalībvalstu VKS un salīdzināti pastāvošie kiberdrošības gatavības modeļi. Pastāvošajiem gatavības modeļiem tika veikta salīdzinošā vērtēšana, izmantojot šim pētījumam īpaši izstrādātu analīzes sistēmu. Analīzes sistēmas pamatā ir Bekera [*Becker*][2] gatavības modeļu izstrādes metodika, kurā ir izklāstīts vispārīgs, konsolidēts

[2] Becker, J., Knackstedt, R., un Pöppelbuß, J., "Developing Maturity Models for IT Management: A Procedure Model and its Application", *Business & Information Systems Engineering*, 1. sēj., Nr. 3, 213.–222. lpp., 2009. gada jūnijs.

gatavības modeļu izstrādes procedūras modelis un norādītas skaidras prasības gatavības modeļu izstrādei. Analīzes sistēma tika papildus pielāgota, lai atbilstu šā pētījuma vajadzībām.

2. **Ekspertu un ieinteresēto personu viedokļu apkopošana**. Šajā posmā, pamatojoties uz dokumentu izpētē savāktajiem datiem un ar tiem saistītajiem analīzē izdarītajiem sākotnējiem konstatējumiem, tika apzināti un uzaicināti uz interviju eksperti ar pieredzi VKS vai gatavības modeļu izstrādē un īstenošanā. *ENISA* sazinājās ar Valsts kiberdrošības stratēģiju ekspertu grupu un valstu sadarbības koordinatoriem (VSK), lai atrastu attiecīgus ekspertus katrā dalībvalstī. Tika intervēti arī daži eksperti, kas ir iesaistīti gatavības modeļu izstrādē. Kopumā tika veiktas 22 intervijas, no kurām 19 ar dažādu dalībvalstu (un EBTA valstu) kiberdrošības aģentūru pārstāvjiem.
3. **Situācijas apzināšanā iegūto datu analīze.** Dokumentu izpētē un intervijās savāktie dati pēc tam tika analizēti, lai apzinātu paraugprakses, kas tiek izmantotas VKS gatavības novērtēšanā izmantojamās pašnovērtēšanas sistēmas izstrādē, izprastu dalībvalstu vajadzības un noteiktu, kurus datus ir praktiski iespējams savākt dažādajās Eiropas valstīs[3]. Šī analīze deva iespēju uzlabot iepriekšējos posmos izstrādāto sākotnējo modeli un precizēt modelī iekļauto rādītāju kopumu, gatavības līmeņus un tā virzienus.
4. **Modeļa pabeigšana.** Valsts spēju pašnovērtēšanas sistēmas atjaunināto versiju pēc tam pārskatīja šajā jomā kompetenti *ENISA* eksperti un tad pirms publicēšanas apstiprināja eksperti 2020. gada oktobra darbseminārā.

1.3 MĒRĶAUDITORIJA

Šis ziņojums ir paredzēts politikas veidotājiem, ekspertiem un valsts ierēdņiem, kas atbild par VKS un plašāk arī par kiberdrošības spēju veidošanu, īstenošanu un izvērtēšanu vai ir iesaistīti šajos uzdevumos. Šajā dokumentā noformētie konstatējumi var noderēt arī kiberdrošības politikas ekspertiem un pētniekiem valsts vai Eiropas līmenī.

[3] Šajā pētījumā ar terminu "Eiropas valstis", kas lietots šajā ziņojumā, ir jāsaprot 27 ES dalībvalstis.

2. KONTEKSTS

2.1 IEPRIEKŠĒJS DARBS VKS DZĪVES CIKLA JOMĀ

Kā norādīts ES Kiberdrošības aktā, viens no *ENISA* galvenajiem mērķiem ir palīdzēt dalībvalstīm izstrādāt valsts tīklu un informācijas sistēmu drošības stratēģijas, veicināt šo stratēģiju izplatīšanu un uzraudzīt to īstenošanu. *ENISA* savu pilnvaru ietvaros ir sagatavojusi vairākus dokumentus par šo tēmu, lai veicinātu dalīšanos labā praksē un sekmētu VKS īstenošanu visā ES:

- 2012. gadā publicētos praktiskos norādījumus "Practical guide on the development and execution phase of NCSS"[4];
- 2012. gadā publicēto dokumentu "Setting the course for national efforts to strengthen security in cyberspace"[5];
- 2014. gadā publicēto *ENISA* pirmo dalībvalsts VKS izvērtēšanas sistēmu[6];
- 2014. gadā publicēto interaktīvo VKS tiešsaistes karti[7];
- 2016. gadā publicētos labas prakses norādījumus "NCSS Good Practice Guide"[8];
- 2018. gadā publicēto Valstu kiberdrošības stratēģiju izvērtēšanas rīku[9];
- 2019. gadā publicēto labas prakses dokumentu "Good practices in innovation on Cybersecurity under the NCSS"[10].

C PIELIKUMĀ "Citi aplūkotie mērķi" ir īsi anotētas *ENISA* galvenās publikācijas par šo tēmu.

Dokumentu izpētē tika izskatīti arī iepriekš minētie norādījumu un citi dokumenti. Īpaši svarīgs VSNS elements ir Valstu kiberdrošības stratēģiju izvērtēšanas rīks[11]. VSNS ir veidota, balstoties uz mērķiem, kas ir iekļauti VKS tiešsaistes izvērtēšanas rīkā.

2.2 EIROPAS VKS KONSTATĒTIE KOPĪGIE MĒRĶI

Dalībvalstu atšķirību dēļ ir grūti noteikt kopīgas darbības vai rīcības plānus atšķirīgajos valstu apstākļos, tiesiskajā regulējumā un politikas programmās. Taču dalībvalstu VKS stratēģiskie

[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] Valstu kiberdrošības stratēģijas — interaktīva karte (*ENISA*, 2014, atjaunināta 2019. gadā), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[8] Ar šo dokumentu tiek atjaunināti 2012. gada norādījumi "NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies" (*ENISA*, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[9] Valstu kiberdrošības stratēģiju izvērtēšanas rīks (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] Valstu kiberdrošības stratēģiju izvērtēšanas rīks (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

mērķi bieži vien attiecas uz vienām un tām pašām tēmām. Tādējādi, pamatojoties uz *ENISA* iepriekšējo darbu un dalībvalstu VKS analīzi, tika noteikti 22 stratēģiskie mērķi. Piecpadsmit no šiem stratēģiskajiem mērķiem *ENISA* jau bija apzinājusi savā iepriekšējā darbā, divi tika pievienoti no jauna šā pētījuma gaitā, bet pieci mērķi tika atlasīti vēlākai izskatīšanai.

2.2.1 Dalībvalstīm kopīgie stratēģiskie mērķi

Pamatojoties uz *ENISA* iepriekš veikto darbu, proti, Valstu kiberdrošības stratēģiju izvērtēšanas rīku[12], nākamajā tabulā ir atspoguļots iepriekš minētais dalībvalstīm kopīgo 15 stratēģisko mērķu kopums, ko tās ir iekļāvušas savās VKS. Mērķuzdevumi atspoguļo, kāds pēc būtības ir valstu redzējums konkrētajā jautājumā. Papildu informāciju par tālāk aprakstītajiem mērķiem skatiet *ENISA* ziņojumā "NCSS Good Practice Guide"[13].

1. tabula. Dalībvalstīm kopīgie stratēģiskie mērķi, ko tās norādījušas savās VKS

ID	VKS stratēģiskie mērķi	Mērķuzdevumi
1	**Izstrādāt valsts ārkārtas rīcības plānus kiberdrošības jomā**	▶ Norādīt un paskaidrot kritērijus, uz kuru pamata situāciju varētu atzīt par krīzi ▶ Noteikt galvenos procesus un darbības krīzes pārvarēšanai ▶ Skaidri noteikt dažādu ieinteresēto personu lomu un pienākumus kiberkrīzē ▶ Norādīt un paskaidrot kritērijus, uz kuru pamata krīzi var atzīt par beigušos, un/vai norādīt, kurš ir pilnvarots pasludināt krīzes beigas
2	**Noteikt pamata drošības pasākumus**	▶ Saskaņot dažādo praksi, ko izmanto publiskā un privātā sektora organizācijas ▶ Radīt kompetentajām publiskā sektora iestādēm un organizācijām kopēju valodu un atvērt drošus komunikācijas kanālus ▶ Dot dažādajām ieinteresētajām personām iespēju pārbaudīt un salīdzināt savas spējas kiberdrošības jomā ▶ Dalīties ar informāciju par kiberdrošības labo praksi visās jomas nozarēs ▶ Palīdzēt ieinteresētajām personām noteikt ieguldījumu prioritātes drošības jomā
3	**Organizēt kiberdrošības mācības**	▶ Noteikt, kas ir jātestē (plāni un procesi, cilvēki, infrastruktūra, reaģēšanas spējas, sadarbības spējas, komunikācija utt.) ▶ Izveidot valsts kiberdrošības mācību plānošanas komandu un dot tai skaidru pilnvarojumu ▶ Integrēt kiberdrošības mācības valsts kiberdrošības stratēģijas vai valsts ārkārtas rīcības plāna kiberdrošības jomā dzīves ciklā
4	**Radīt spējas reaģēt uz incidentiem**	▶ Pilnvarojums — tas attiecas uz pilnvarām, lomu un pienākumiem, kas attiecīgajai valdībai ir jāpiešķir komandai ▶ Pakalpojumu portfelis — tas ietver pakalpojumus, ko komanda sniedz savam klientu lokam vai izmanto savas iekšējās darbības nodrošināšanai ▶ Darbības spējas — tās attiecas uz tehniskajām un darbības prasībām, kuras komandai ir jāievēro ▶ Sadarbības spējas — tās aptver iepriekšējās trīs kategorijās neietilpstošas prasības par informācijas kopīgošanu ar citām komandām, piemēram, politikas veidotājiem, militārpersonām, regulētājiem, (informācijas kritiskās infrastruktūras) operatoriem, tiesībaizsardzības iestādēm

[12] Valstu kiberdrošības stratēģiju izvērtēšanas rīks (2018), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.
[13] Ar šo dokumentu tiek atjaunināti 2012. gada norādījumi "NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies" (*ENISA*, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

ID	VKS stratēģiskie mērķi	Mērķuzdevumi
5	Vairot lietotāju izpratni	▶ Noteikt nepilnības zināšanās par kiberdrošības vai informācijas drošības jautājumiem ▶ Novērst šīs nepilnības, vairojot izpratni vai pilnveidojot/nostiprinot zināšanu bāzi
6	Stiprināt apmācības un izglītības programmas	▶ Uzlabot informācijas drošības jomā pašlaik strādājošo personu darbības spējas ▶ Mudināt studentus pievienoties un tad sagatavot viņus iesaistei kiberdrošības jomā ▶ Veicināt un rosināt attiecības starp informācijas drošības jomas akadēmisko vidi un informācijas drošības jomas nozari ▶ Saskaņot kiberdrošības jomā nodrošināto apmācību ar uzņēmumu vajadzībām
7	Veicināt PI	▶ Noteikt ievainojamību patiesos cēloņus, nevis vienkārši novērst to sekas ▶ Sapulcēt dažādu disciplīnu zinātniekus, lai tie sniegtu risinājumus daudzšķautņainām un kompleksām problēmām, piemēram, kiberfiziskiem draudiem ▶ Sasaistīt nozares vajadzības ar pētniecības rezultātiem, tādējādi atvieglojot pāreju no teorijas uz praksi ▶ Atrast veidus, kā ne tikai saglabāt, bet arī paaugstināt to produktu un pakalpojumu kiberdrošības līmeni, kas tiek izmantoti pastāvošajās kiberinfrastruktūrās
8	Dot privātajam sektoram stimulus ieguldīt drošības pasākumos	▶ Noteikt stimulus, kas varētu pamudināt privātus uzņēmumus veikt ieguldījumus drošības pasākumos ▶ Sniegt uzņēmumiem stimulus, lai veicinātu ieguldījumus drošībā
9	Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus (IKI)	▶ Apzināt informācijas kritisko infrastruktūru ▶ Apzināt un mazināt attiecīgus riskus, ar ko saskaras IKI
10	Apkarot kibernoziedzību	▶ Izveidot tiesību aktus kibernoziedzības jomā ▶ Vairot tiesībaizsardzības iestāžu efektivitāti
11	Izveidot mehānismus ziņošanai par incidentiem	▶ Gūt zināšanas par draudu kopainu ▶ Novērtēt incidentu (piem., drošības prasību pārkāpumu, tīkla kļūmju, pakalpojumu pārtraukumu) ietekmi ▶ Gūt zināšanas par pastāvošām un jaunām neaizsargātībām un uzbrukumu veidiem ▶ Attiecīgi atjaunināt drošības pasākumus ▶ Īstenot TID direktīvas noteikumus, kas attiecas uz ziņošanu par incidentiem
12	Pastiprināt privātuma un datu aizsardzību	▶ Sniegt ieguldījumu ar privātumu un datu aizsardzību saistīto pamattiesību nostiprināšanā
13	Izveidot publiskā un privātā sektora partnerību (PPP)	▶ Atturēšana (atturēt uzbrucējus) ▶ Aizsargāšana (izmanto pētījumus par jauniem drošības apdraudējumiem) ▶ Atklāšana (dalās ar informāciju, lai novērstu jaunus draudus) ▶ Reaģēšana (nodrošināt spējas tikt galā ar incidenta sākotnējo ietekmi) ▶ Atkopšana (nodrošināt spējas vērst par labu incidenta galīgo ietekmi)
14	Institucionalizēt sadarbību starp publiskā sektora aģentūrām	▶ Pastiprināt sadarbību starp publiskā sektora aģentūrām, kas ir atbildīgas un kompetentas kiberdrošības jautājumos ▶ Izvairīties no kompetenču un resursu pārklāšanās publiskā sektora aģentūru starpā ▶ Uzlabot un institucionalizēt sadarbību starp publiskā sektora aģentūrām dažādās kiberdrošības jomās
15	Iesaistīties starptautiskajā sadarbībā (ne tikai ar ES dalībvalstīm)	▶ Gūt labumu no kopīgas zināšanu bāzes izveides ES dalībvalstu starpā ▶ Radīt sinerģiju starp valstu kiberdrošības iestādēm ▶ Dot iespēju cīnīties pret pārrobežu noziedzību un pastiprināt šo cīņu

2.2.2 Papildu stratēģiskie mērķi

Pamatojoties uz veikto dokumentu izpēti un *ENISA* īstenotajām intervijām, tika noteikti papildu stratēģiskie mērķi. Dalībvalstis aizvien vairāk pievēršas šiem jautājumiem savās VKS vai nosaka rīcības plānus šajos jautājumos. Ir sniegti arī dalībvalstu īstenoto darbību piemēri. Ja piemērs ir iegūts no publiski pieejama avota, ir sniegta atsauce. Ja piemēri ir iegūti no konfidenciālām intervijām ar ES dalībvalstu ierēdņiem, atsauces nav dotas.

Tika konstatēti šādi papildu stratēģiskie mērķi:

- uzlabot piegādes ķēdes kiberdrošību un
- nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem.

Uzlabot piegādes ķēdes kiberdrošību

Mazie un vidējie uzņēmumi (MVU) ir Eiropas ekonomikas mugurkauls. Tādu ir 99 % no visiem uzņēmumiem ES[14], un 2015. gadā tika lēsts, ka MVU ir radījuši aptuveni 85 % no jaunajām darbvietām un divas trešdaļas no kopējās nodarbinātības privātajā sektorā ES. Turklāt, tā kā MVU sniedz pakalpojumus lieliem uzņēmumiem un aizvien vairāk sadarbojas ar valsts pārvaldes iestādēm[15], jāņem vērā, ka mūsdienu savienotajā pasaulē MVU ir vājais posms aizsardzībā pret kiberuzbrukumiem. MVU patiešām ir visvairāk neaizsargāti pret kiberuzbrukumiem, taču bieži vien tie nevar atļauties veikt pietiekami lielus ieguldījumus kiberdrošībā[16]. Tāpēc piegādes ķēdes kiberdrošības uzlabošanā lielākā uzmanība būtu jāpievērš MVU.

Dalībvalstis var ne tikai izmantot šo sistēmisko pieeju, bet arī pastiprināt centienus konkrētu tādu IKT pakalpojumu un produktu kiberdrošības jomā, kuri tiek uzskatīti par būtiskiem; to vidū var minēt IKT tehnoloģijas, kas tiek izmantotas informācijas kritiskajā infrastruktūrā, drošības mehānismus, kas tiek piemēroti telesakaru nozarē (interneta pakalpojumu sniedzēju kontroles u. c.), uzticamības pakalpojumus, kas definēti *eIDAS* regulā, un mākoņpakalpojumu sniedzējus. Piemēram, Polija savā valsts kiberdrošības stratēģijā 2019.–2024. gadam[17] apņēmās izstrādāt valsts kiberdrošības novērtēšanas un sertifikācijas sistēmu kā mehānismu, ar kuru nodrošināt kvalitāti piegādes ķēdē. Šī sertifikācijas sistēma būs saskaņota ar IKT digitālajiem produktiem, pakalpojumiem un procesiem paredzēto ES sertifikācijas satvaru, kas izveidots ar ES Kiberdrošības aktu (Regulu (ES) 2019/881).

Tātad ir ārkārtīgi svarīgi uzlabot piegādes ķēdes kiberdrošību. To var panākt, izveidojot spēcīgu politiku MVU darbības veicināšanai, nodrošinot pamatnostādnes par kiberdrošības prasībām valsts pārvaldes iestāžu iepirkuma procedūrās, veicinot sadarbību privātajā sektorā, veidojot PPP, popularizējot koordinētas ievainojamību atklāšanas (*CVD*) mehānismus[18], veidojot produktu sertifikācijas shēmu, iekļaujot kiberdrošības komponentus MVU paredzētās digitālās iniciatīvās, finansējot spēju pilnveidi utt.

Nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem

Komisija 2020. gada februāra paziņojumā "Eiropas digitālās nākotnes veidošana"[19] izklāstīja savu redzējumu par tādu ES digitālo pārveidi, kuras mērķis būtu nodrošināt iekļaujošas

[14] https://ec.europa.eu/growth/smes/.
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm.
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study.
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf.
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.
[19] "Eiropas digitālās nākotnes veidošana", COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf.

tehnoloģijas, kas darbojas cilvēku labā, un kurā tiktu ievērotas ES pamatvērtības. Jo īpaši paziņojumā ir norādīts, ka izšķirīga nozīme ir valstu pārvaldes iestāžu digitālās pārveides veicināšanai visā Eiropā. Tāpēc ir ārkārtīgi svarīgi vairot uzticību valdībai attiecībā uz digitālo identitāti un uzticību publiskajiem pakalpojumiem. Tas ir vēl jo svarīgāk tāpēc, ka darījumiem un datu apmaiņai publiskajā sektorā bieži vien ir sensitīvs raksturs.

Daudz valstu ir paudušas nodomu pievērsties šim tematam savā VKS, piemēram, Dānija, Igaunija, Francija, Luksemburga, Malta, Spānija, Nīderlande un Apvienotā Karaliste. Dažas no šīm valstīm ir arī norādījušas, ka šim stratēģiskajam mērķim varētu pievērsties plašāka plāna kontekstā:

- Igaunija savu rīcības plānu šajā jautājumā "Elektroniskās identitātes drošība un elektroniskās autentifikācijas spējas" sasaista ar plašāko Igaunijas Digitālo programmu 2020. gadam;
- Francijas VKS ir norādīts, ka par digitālajām tehnoloģijām atbildīgais valsts sekretārs pārrauga ceļveža, kas paredzēts, "lai aizsargātu Francijas iedzīvotāju digitālo dzīvi, privātumu un persondatus", izveidi;
- Nīderlandes VKS ir norādīts, ka kiberdrošība valsts pārvaldes iestādēs, kā arī iedzīvotājiem un uzņēmumiem nodrošinātajos publiskajos pakalpojumos ir sīkāk aplūkoti Plašajā digitālās pārvaldes programmā;
- tā kā Apvienotās Karalistes valdība turpina aizvien vairāk savu pakalpojumu pārcelt uz interneta vidi, tā ir uzdevusi Valdības digitālajam dienestam (*GDS*) ar Apvienotās Karalistes Nacionālā kiberdrošības centra (*NSCS*) atbalstu nodrošināt, ka visi jaunie digitālie pakalpojumi, ko valdība izveido vai iegādājas, ir arī "droši pēc noklusējuma".

2.2.3 Citi apsvērtie stratēģiskie mērķi

Dokumentu izpētes posmā un *ENISA* īstenotajās intervijās tika aplūkoti vēl citi stratēģiskie mērķi. Tomēr tika nolemts šos mērķus neiekļaut pašnovērtēšanas sistēmā. C PIELIKUMS. Citi aplūkotie mērķi

ir definēts katrs no šiem mērķiem, ko var izmantot, lai rosinātu turpmākas diskusijas par iespējamiem VKS uzlabojumiem.

Turpmākai apsvēršanai tika aplūkoti šādi stratēģiskie mērķi:

- izstrādāt nozaru kiberdrošības stratēģijas;
- apkarot dezinformācijas kampaņas;
- nodrošināt augstās tehnoloģijas (5G, *AI*, kvantisko datošanu u. c.);
- nodrošināt datu suverenitāti;
- stimulēt kiberapdrošināšanas nozares attīstību.

2.3 SALĪDZINOŠAJĀ VĒRTĒŠANĀ GŪTĀS GALVENĀS ATZIŅAS

Dokumentu izpēte, kurā tika aplūkoti pastāvošie ar kiberdrošību saistītie gatavības modeļi, tika veikta, lai ievāktu informāciju un pierādījumus, uz kuriem balstīties, izstrādājot valsts spēju pašnovērtēšanas sistēmu VKS jomā. Šajā saistībā tika izskatīts daudz literatūras avotu par pastāvošajiem modeļiem, lai papildinātu konstatējumus, kas tika izdarīti sākotnējā darbības jomas izpētē par kiberdrošības gatavības noteikšanas modeļiem un pastāvošajām VKS, un šis veikums ir sīkāk aprakstīts 2.1. un 2.2. iedaļā. Sistemātiskajā apskatā gūtā informācija palīdzēja izvēlēties un pamatot novērtēšanas sistēmas gatavības līmeņus, kā arī noteikt dažādos virzienus un rādītājus.

Gatavības noteikšanas modeļu sistemātiskajā apskatā tika aplūkoti 10 modeļi, kas tika analizēti pēc to galvenajiem elementiem. Vispārīgs pārskats par katra šajā pētījumā apskatītā modeļa galvenajiem elementiem ir pieejams 2. tabulā "Pārskats par analizētajiem gatavības modeļiem", bet detalizētāka analīze ir izklāstīta A PIELIKUMĀ.

2. tabula. Pārskats par analizētajiem gatavības modeļiem

Modeļa nosaukums	Gatavības līmeņu skaits	Atribūtu skaits	Novērtēšanas metode	Rezultātu atspoguļojums
Kiberdrošības spēju gatavības modelis valstīm (*CMM*)	5	5 galvenie virzieni	Sadarbība ar vietējo organizāciju, lai precizētu modeli pirms tā piemērošanas valsts kontekstā	Radardiagramma ar 5 sektoriem
Kiberdrošības spēju gatavības modelis (*C2M2*)	4	10 galvenās jomas	Pašizvērtēšanas metodika un rīkkopa	Rādītāju sistēma ar sektoru diagrammām
Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēma	n. p. (4 līmeņi)	5 pamatfunkcijas	Pašnovērtējums	n. p.
Kataras kiberdrošības spēju gatavības modelis (*Q-C2M2*)	5	5 galvenās jomas	n. p.	n. p.
Kiberdrošības gatavības modeļa sertifikācija (*CMMC*)	5	17 galvenās jomas	Ārēju revidentu veikts novērtējums	n. p.
Pašvaldību kiberdrošības gatavības modelis (*CCSMM*)	5	6 galvenie virzieni	Pašvaldības veikts novērtējums, kurā ieguldījumu sniedz štata un federālās tiesībaizsardzības iestādes	n. p.
Informācijas drošības gatavības modelis *NIST* kiberdrošības satvaram (*ISMM*)	5	23 vērtētas jomas	n. p.	n. p.
Iekšējās revīzijas spēju modelis (*IA-CM*) publiskajam sektoram	5	6 elementi	Pašnovērtējums	n. p.
Globālais kiberdrošības indekss (*GCI*)	n. p.	5 pīlāri	Pašnovērtējums	Rangu tabula
Kiberspēcīguma indekss (CPI)	n. p.	4 kategorijas	“Economist Intelligence Unit” veikta salīdzinošā vērtēšana	Rangu tabula

Šis sistemātiskais apskats deva iespēju izdarīt secinājumus par pastāvošajos modeļos izmantoto paraugpraksi, kas palīdzēja izstrādāt šā gatavības modeļa koncepciju. Konkrētāk, veiktā salīdzinošā vērtēšana palīdzēja definēt gatavības līmeņus, izveidot virzienu grupas un atlasīt rādītājus, kā arī izvēlēties atbilstošu vizualizācijas metodiku modeļa rezultātiem. Visbūtiskākie konstatējumi par katru no šiem elementiem ir izklāstīti 3. tabulā.

3. tabula. Salīdzinošajā vērtēšanā gūtās galvenās atziņas

Elements	Galvenās atziņas
Gatavības līmeņi	▶ Kiberdrošības spēju novērtēšanas sistēmās parasti tiek pieņemta piecu līmeņu gatavības skala, kas spēj nodrošināt detalizētus novērtējuma rezultātus (izsmeļošu pārskatu par katra modeļa gatavības līmeņu definīciju sk. 6. tabulā "Gatavības līmeņu salīdzinājums"). ▶ Visos modeļos ir sniegta katra gatavības līmeņa vispārīga definīcija, kas pēc tam tiek pielāgota dažādajiem virzieniem vai virzienu grupām. ▶ Mērot kiberdrošības spēju gatavību, parasti tiek novērtēti divi galvenie aspekti — stratēģiju gatavība un stratēģiju īstenošanas vajadzībām ieviesto procesu gatavība.
Atribūti	▶ Pastāvošo gatavības modeļu atribūtu salīdzinošajā analīzē gūti neviendabīgi rezultāti un konstatēts, ka vienam modelim vidēji ir četri vai pieci atribūti. ▶ Modelis, kas balstās uz aptuveni četriem vai pieciem atribūtiem, sniedz valstīm pietiekami detalizētus datus, sagrupējot kopā atbilstošus virzienus un nodrošinot, ka rezultāti ir viegli saprotami (katra modeļa atribūtu aprakstu sk. 7. tabulā "Atribūtu/virzienu salīdzinājums"). ▶ Galvenais princips, pēc kura visos modeļos tiek veidotas grupas, ir grupā apvienot saskaņotus elementus.
Novērtēšanas metode	▶ Dažādajos analizētajos modeļos izmantotās novērtēšanas metodes ir atšķirīgas. ▶ Visbiežāk izmantotā novērtēšanas metode balstās uz pašizvērtēšanu.
Rezultātu atspoguļojums	▶ Ir svarīgi rezultātus atspoguļot atšķirīgās detalizācijas pakāpēs. ▶ Vizualizācijas metodikai vajadzētu būt tādai, lai vizualizācija būtu skaidri saprotama un viegli nolasāma.

Konceptuālais modelis tika veidots, pamatojoties uz dažādo gatavības modeļu salīdzinošo vērtējumu, kā arī *ENISA* iepriekš veikto darbu. Tika arī nolemts izmantot *ENISA interaktīvo tiešsaistes rīku*, lai izstrādātu gatavības rādītājus katram atribūtam.

2.4 VKS IZVĒRTĒŠANAS PROBLĒMAS

Dalībvalstis saskaras ar daudzām problēmām, kad tās veido kiberdrošības spējas, jo īpaši, kad tās cenšas nodrošināt, ka to spējas atbilst jaunākajiem pavērsieniem. Tālāk ir rezumētas problēmas, ko dalībvalstis norādīja un kas ar tām tika apspriestas šajā pētījumā.

- **Ar koordināciju un sadarbību saistītas grūtības.** Koordinēt kiberdrošības pasākumus valsts līmenī, lai varētu efektīvi reaģēt uz kiberdrošības problēmām, var būt grūti, jo tajos ir iesaistīts daudz ieinteresēto personu.
- **Resursu trūkums novērtējuma veikšanai.** Atkarībā no vietējiem apstākļiem un kiberdrošības pārvaldības struktūras valstī VKS un tās mērķu izvērtēšanai var būt vajadzīgs pat vairāk par 15 cilvēkdienām.
- **Atbalsta trūkums kiberdrošības spēju attīstīšanai.** Dažas dalībvalstis norādīja — lai tās varētu pamatot nepieciešamo budžetu un saņemt atbalstu kiberdrošības spēju attīstīšanai, tām vispirms ir jāīsteno izvērtēšanas posms, lai noteiktu nepilnības un ierobežojumus.
- **Grūtības panākumu vai pārmaiņu attiecināšanā uz stratēģiju.** Tā kā apdraudējumi ar katru dienu aizvien attīstās un tehnoloģijas uzlabojas, rīcības plāni ir nepārtraukti jāpielāgo, lai uz to reaģētu. Taču VKS izvērtēšana un pārmaiņu attiecināšana uz stratēģiju ir grūts uzdevums. Savukārt tas apgrūtina VKS ierobežojumu un trūkumu apzināšanu.
- **Grūtības novērtēt VKS efektivitāti.** Var savākt rādījumus, lai izmērītu dažādas jomas, piemēram, progresu, īstenošanu, gatavību un efektivitāti. Lai gan izmērīt progresu un

īstenošanu ir salīdzinoši vieglāk nekā efektivitāti, tieši efektivitātes mērījumi sniedz skaidrāku priekšstatu par VKS iznākumiem un ietekmi. *ENISA* īstenotajās intervijās daudz dalībvalstu norādīja, ka ir svarīgi kvantitatīvi mērīt VKS efektivitāti, bet tas ir arī ļoti grūts uzdevums, kas dažos gadījumos praktiski nav pat paveicams.

- **Grūtības vienotas sistēmas pieņemšanā.** ES dalībvalstis darbojas dažādos apstākļos — atšķiras gan to politika, gan arī organizācijas, kultūra, sabiedrības struktūra un VKS gatavība. Dažas no šajā pētījumā intervētajām dalībvalstīm norādīja, ka varētu būt grūti pamatot un izmantot universālu pašnovērtēšanas sistēmu.

2.5 VALSTS SPĒJU NOVĒRTĒŠANAS LABUMS

Visām ES dalībvalstīm kopš 2017. gada ir sava VKS[20]. Tas ir pozitīvi, tomēr ir arī svarīgi, lai dalībvalstis spētu pienācīgi novērtēt šīs VKS un tādējādi sniegt pievienoto vērtību savai stratēģiskajai plānošanai un stratēģijas īstenošanai.

Viens no valsts spēju novērtēšanas sistēmas mērķiem ir izvērtēt kiberdrošības spējas, pamatojoties uz dažādajās VKS izklāstītajām prioritātēm. Pamatā ar sistēmu tiek novērtēts dalībvalstu kiberdrošības spēju gatavības līmenis tajās jomās, kas ir noteiktas VKS mērķos. Tādējādi ar sistēmu veiktā novērtējuma rezultāti palīdz dalībvalstu politikas veidotājiem formulēt valsts kiberdrošības stratēģiju, jo sniedz tiem informāciju par pašreizējo situāciju valstī[21]. VSNS galvenais mērķis ir palīdzēt dalībvalstīm noteikt, kurās jomās ir nepieciešami uzlabojumi, un veidot spējas.

Sistēmas mērķis ir dot dalībvalstīm iespēju pašām novērtēt savu gatavības līmeni, novērtējot savus VKS mērķus, un tādējādi palīdzēt tām uzlabot un veidot kiberdrošības spējas gan stratēģiskā, gan operatīvā līmenī.

Praktiskākā ziņā, pamatojoties uz intervijām, ko *ENISA* īstenoja ar vairākām aģentūrām, kuras atbild par kiberdrošības jomu dažādās dalībvalstīs, tika noteikts un uzsvērts, ka valsts spēju novērtēšanas sistēma dod šādus labumus:

- sniedz noderīgu informāciju, kas palīdz izstrādāt ilgtermiņa stratēģiju (piem., laba prakse, pamatnostādnes);
- palīdz atklāt, kādu elementu VKS vēl trūkst;
- palīdz turpināt veidot kiberdrošības spējas;
- palīdz nodrošināt pārskatatbildību par politisko rīcību;
- vairo plašas sabiedrības un starptautisko partneru uzticību;
- palīdz labāk uzrunāt auditoriju un veidot pārredzamas organizācijas tēlu sabiedrībā;
- palīdz paredzēt gaidāmās problēmas;
- palīdz apzināt gūtās mācības un paraugpraksi;
- sniedz priekšstatu par kiberdrošības spēju kopējo līmeni ES, lai atvieglotu diskusijas;
- palīdz izvērtēt valsts spējas kiberdrošības jomā.

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

3. VALSTS SPĒJU NOVĒRTĒŠANAS SISTĒMAS METODIKA

3.1 VISPĀRĪGAIS MĒRĶIS

VSNS **galvenais mērķis** ir novērtēt **dalībvalstu** kiberdrošības spēju gatavības līmeni, lai palīdzētu tām izvērtēt savas valsts kiberdrošības spējas, uzlabot informētību par valsts gatavības līmeni, noteikt jomas, kurās nepieciešami uzlabojumi, un veidot kiberdrošības spējas.

3.2 GATAVĪBAS LĪMEŅI

Sistēmas pamatā ir **pieci gatavības līmeņi**, kas atspoguļo posmus, kurus dalībvalstis īsteno, veidojot kiberdrošības spējas katrā VKS mērķī ietvertajā jomā. Ar katru minēto līmeni gatavības pakāpe aizvien paaugstinās, sākot no **1. līmeņa**, kurā dalībvalstīm nav skaidri noteiktas pieejas kiberdrošības spēju veidošanai VKS mērķos ietvertajās jomās, un beidzot ar **5. līmeni**, kurā kiberdrošības spēju veidošanas stratēģija ir dinamiska un pielāgojas izmaiņām apkārtējā vidē. 4. tabulā ir parādīta gatavības līmeņu skala un aprakstīts katrs gatavības līmenis.

4. tabula. *ENISA* valsts spēju novērtēšanas sistēmas piecu līmeņu gatavības skala

1. LĪMENIS — SĀKOTNĒJAIS / *AD HOC* POSMS	2. LĪMENIS — IEVIEŠANAS SĀKUMPOSMS	3. LĪMENIS — NOSTIPRINĀŠANĀS	4. LĪMENIS — OPTIMIZĀCIJA	5. LĪMENIS — ADAPTĪVAIS POSMS
Dalībvalstij nav skaidri noteiktas pieejas kiberdrošības spēju veidošanai VKS mērķos ietvertajās jomās. Tomēr valstij var būt noteikti daži vispārīgi mērķi, un tā var būt veikusi dažus (tehniskus, politiskus, pamatnostādņu) pētījumus, lai uzlabotu valsts spējas.	Ir noteikta valsts pieeja spēju veidošanai VKS mērķos ietvertajā jomā. Ir ieviesti rezultātu sasniegšanai nepieciešamie rīcības plāni vai pasākumi, tomēr tie vēl ir sākotnējā posmā. Var būt arī apzinātas un/vai iesaistītas aktīvas ieinteresētās personas.	Ir skaidri noteikts rīcības plāns spēju veidošanai VKS mērķos ietvertajā jomā, un to atbalsta attiecīgās ieinteresētās personas. Prakse un pasākumi tiek piemēroti un īstenoti vienveidīgi visā valstī. Pasākumi ir noteikti un dokumentēti, un tiem ir skaidri noteikts resursu piešķīrums un pārvaldība, kā arī termiņi.	Rīcības plānu regulāri novērtē; tam tiek noteiktas prioritātes, tas tiek optimizēts un ir ilgtspējīgs. Kiberdrošības spēju veidošanas pasākumu rezultātus regulāri novērtē. Tiek noteikti panākumu faktori, grūtības un nepilnības pasākumu īstenošanā.	Kiberdrošības spēju veidošanas stratēģija ir dinamiska un adaptīva. Tā kā pastāvīgi tiek pievērsta uzmanība pārmaiņām apkārtējā vidē (tehnoloģiju progresam, konfliktiem pasaulē, jauniem apdraudējumiem utt.), ir iespējams ātri pieņemt lēmumus un ātri rīkoties, lai panāktu uzlabojumus.

3.3 PAŠNOVĒRTĒŠANAS SISTĒMAS GRUPAS UN PAMATSTRUKTŪRA

Pašnovērtēšanas sistēmai ir **četras grupas**: I) kiberdrošības pārvaldība un standarti; II) spēju veidošana un izpratnes vairošana; III) juridiskie un normatīvie jautājumi un IV) sadarbība. Katra no šīm grupām atspoguļo būtisku tematisko jomu, kurā jāveido kiberdrošības spējas valstī, un ietver dažādu tādu mērķu kopumu, ko dalībvalstis var iekļaut savās VKS. Konkrēti:

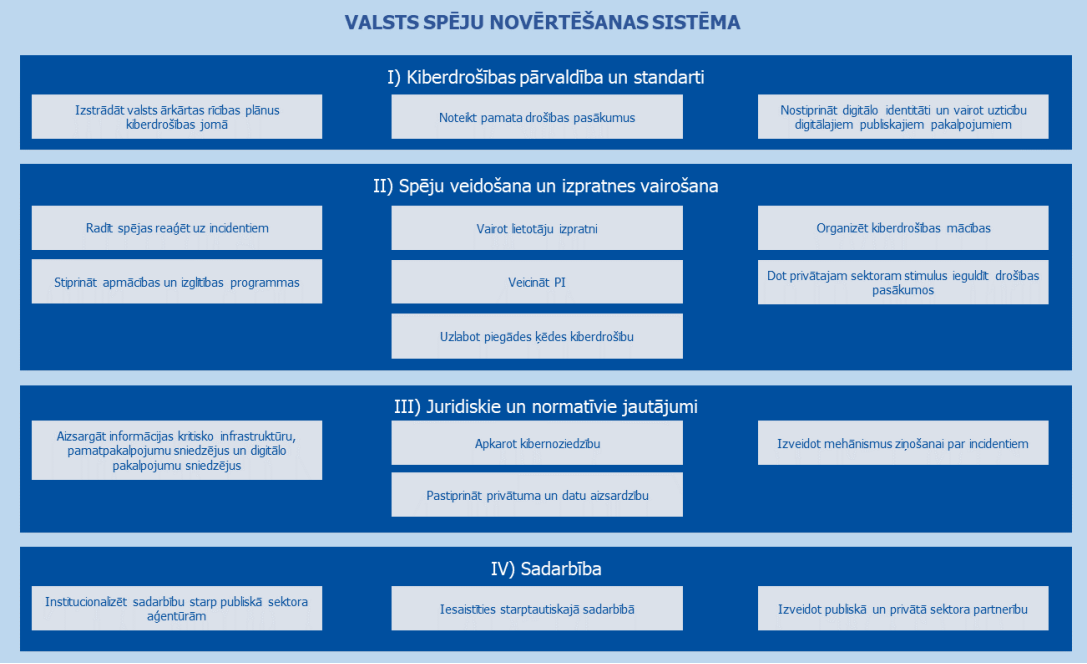
- **(I) kiberdrošības pārvaldība un standarti**: šajā grupā tiek mērīta dalībvalstu spēja ieviest pienācīgu pārvaldību, standartus un labu praksi kiberdrošības jomā. Šajā virzienā ir aplūkoti dažādi kiberaizsardzības un noturības aspekti, un tas palīdz attīstīt valsts kiberdrošības nozari un vairot uzticību valdībām;
- **(II) spēju veidošana un izpratnes vairošana**: šajā grupā tiek novērtētas dalībvalstu spējas vairot izpratni par kiberdrošības riskiem un apdraudējumiem un to novēršanas paņēmieniem. Šajā virzienā tiek arī novērtēta valsts spēja pastāvīgi veidot kiberdrošības spējas un paaugstināt zināšanu un prasmju kopējo līmeni šajā jomā. Tas pievēršas kiberdrošības tirgus attīstībai un progresam kiberdrošības pētniecībā un izstrādē. Šajā grupā ir sagrupēti visi mērķi, kas liek pamatus spēju veidošanas veicināšanai;
- **(III) juridiskie un normatīvie jautājumi**: šajā grupā tiek mērītas dalībvalstu spējas ieviest juridiskos un normatīvos instrumentus, kas nepieciešami, lai novērstu kibernoziedzību un ar to saistītos kiberincidentus un cīnītos pret to apmēra pieaugumu, kā arī aizsargātu informācijas kritisko infrastruktūru. Šajā virzienā tiek arī novērtētas dalībvalstu spējas izveidot tādu tiesisko regulējumu, kas aizsargātu iedzīvotājus un uzņēmumus, piemēram, tā, lai tiktu rasts līdzsvars starp drošību un privātumu;
- **(IV) sadarbība**: šajā grupā tiek izvērtēta sadarbība un informācijas kopīgošana starp dažādām ieinteresēto personu grupām valsts un starptautiskā līmenī — svarīgi rīki, kas ļauj labāk izprast nepārtraukti mainīgo apdraudējumu kopainu un reaģēt uz tiem.

Modelī ir iekļauti tie mērķi, ko dalībvalstis parasti sev noteikušas, un tie ir izvēlēti no 2.2. iedaļā uzskaitīto mērķu vidus. Konkrētāk, modelī tiek novērtēti šādi mērķi.

- 1. Izstrādāt valsts ārkārtas rīcības plānus kiberdrošības jomā (I)
- 2. Noteikt pamata drošības pasākumus (I)
- 3. Nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem (I)
- 4. Radīt spējas reaģēt uz incidentiem (II)
- 5. Vairot lietotāju izpratni (II)
- 6. Organizēt kiberdrošības mācības (II)
- 7. Stiprināt apmācības un izglītības programmas (II)
- 8. Veicināt PI (II)
- 9. Dot privātajam sektoram stimulus ieguldīt drošības pasākumos (II)
- 10. Uzlabot piegādes ķēdes kiberdrošību (II)
- 11. Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus (III)
- 12. Apkarot kibernoziedzību (III)
- 13. Izveidot mehānismus ziņošanai par incidentiem (III)
- 14. Pastiprināt privātuma un datu aizsardzību (III)
- 15. Institucionalizēt sadarbību starp publiskā sektora aģentūrām (IV)
- 16. Iesaistīties starptautiskajā sadarbībā (IV)
- 17. Izveidot publiskā un privātā sektora partnerību (IV)

Visas četras grupas un tām pamatā esošie mērķi ir apvienoti modelī tā, lai sniegtu visaptverošu pārskatu par dalībvalstu kiberdrošības spēju gatavību. 1. attēlā ir atainota pašnovērtēšanas sistēmas pamatstruktūra un parādīts, kā šie elementi — mērķi, grupas un pašnovērtēšanas sistēma — ir saistīti ar valsts rezultātu izvērtēšanu.

1. attēls. Pašnovērtēšanas sistēmas struktūra



Katram pašnovērtēšanas sistēmā iekļautajam mērķim ir norādīti vairāki rādītāji pa pieciem gatavības līmeņiem. Katrs rādītājs ir balstīts uz dihotomu ("jā/nē") jautājumu. Rādītājs var būt obligāts vai neobligāts.

3.4 VĒRTĒJUMA PIEŠĶIRŠANAS MEHĀNISMS

Pašnovērtēšanas sistēmas **vērtējuma piešķiršanas mehānismā** tiek ņemti vērā iepriekš minētie elementi un 3.5. iedaļā uzskaitītie principi. Faktiski modelis sniedz vērtējumu, pamatojoties uz divu parametru — **gatavības līmeņa** un **aptvēruma pakāpes** — vērtību. Katru no šiem parametriem var aprēķināt dažādos līmeņos — i) par katru mērķi, ii) par katru mērķu grupu vai iii) kopumā.

Vērtējumi mērķa līmenī

Gatavības līmeņa vērtējums sniedz pārskatu par gatavības līmeni, parādot, kādas spējas un prakses ir ieviestas. Gatavības līmeņa vērtējumu aprēķina kā visaugstāko līmeni, kurā respondents ir apmierinājis visas obligātās prasības (t. i., atbildējis ar "JĀ" uz visiem obligātajiem jautājumiem) ar noteikumu, ka ir apmierinātas arī visas iepriekšējo gatavības līmeņu obligātās prasības.

Aptvēruma pakāpe parāda, uz cik lielu daļu no visiem rādītājiem ir atbildēts apstiprinoši neatkarīgi no to līmeņa. Tā ir papildvērtība, kurā ir ņemti vērā visi rādītāji, ar ko mēra konkrētu mērķi. Aptvēruma pakāpi rēķina kā attiecību starp attiecīgā mērķa jautājumu kopskaitu un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši.

Svarīgi — tālāk dokumentā ar vārdu "***vērtējums***" tiek apzīmētas gan gatavības līmeņa, gan aptvēruma pakāpes vērtības.

2. attēlā "Mehānisms vērtējuma piešķiršanai pa mērķiem" ir vizualizēts 3.1. iedaļā aprakstītais izvērtēšanas mehānisms, kas tiks sīkāk iztirzāts tālāk tekstā.

2. attēls. Mehānisms vērtējuma piešķiršanai pa mērķiem

2. attēlā sniegtais piemērs parāda, kā tiek aprēķināts gatavības līmenis attiecībā uz konkrētu mērķi. Ievērojiet, ka respondents ir izpildījis visas pirmo trīs gatavības līmeņu obligātās prasības un tikai daļu 4. līmeņa obligāto prasību. Tāpēc vērtējumā ir norādīts, ka ***respondenta gatavības līmenis mērķim "Organizēt kiberdrošības mācības" ir 3. līmenis****.*

Taču 2. attēlā sniegtajā piemērā attiecīgā mērķa gatavības līmenis nespēj atspoguļot to informāciju, ko sniedz rādītāji, kuriem ir pozitīvs vērtējums un kuru gatavības līmenis ir augstāks par trešo. Šādā gadījumā aptveruma pakāpe var sniegt pārskatu par visiem elementiem, ko respondents ir ieviesis, lai sasniegtu minēto mērķi, neraugoties uz tā faktisko gatavības līmeni. Šajā gadījumā attiecība starp attiecīgā mērķa jautājumu kopskaitu un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši, ir 19/27, t. i., ***aptveruma pakāpes vērtība ir 70 %****.*

Papildus tam, lai pielāgotos dalībvalstu specifikai, bet tai pašā laikā arī spētu sniegt konsekventu pārskatu, vērtējumu aprēķina, pamatojoties uz divām dažādām izlasēm, grupas līmenī un kopumā:

- **vispārējie vērtējumi:** viena pilna izlase, kas aptver visus konkrētā grupā vai sistēmā kopumā ietvertos mērķus (no 1 līdz 17);
- **konkrētie vērtējumi:** viena specifiska izlase, kas aptver tikai tos mērķus, ko dalībvalsts atlasījusi konkrētajā grupā vai sistēmā kopumā (tie parasti ir konkrētās valsts VKS ietvertie mērķi).

Vērtējumi grupas līmenī

Katras grupas vispārējo gatavības līmeni aprēķina kā visu attiecīgās grupas mērķu gatavības līmeņa aritmētisko vidējo.

Katras grupas konkrēto gatavības līmeni aprēķina kā to grupas mērķu gatavības līmeņa aritmētisko vidējo, kurus dalībvalsts ir izvēlējusies novērtēt (parasti tie ir konkrētās valsts VKS ietvertie mērķi).

Piemēram, 1. attēlā ir parādīts, ka I grupa "Kiberdrošības pārvaldība un standarti" sastāv no trim mērķiem. Ja pieņem, ka respondents ir izvēlējies novērtēt tikai pirmos divus mērķus, bet trešo ne un ka pirmo divu mērķu gatavības līmenis ir attiecīgi 2. un 4., tad grupas gatavības līmenis, ja ņem vērā visus mērķus, ir 2. (I grupas vispārējais gatavības līmenis = (2 +4) / 3), bet, ja ņem vērā tikai novērtētāja izvēlētos konkrētos mērķus, tad grupas gatavības līmenis ir 3. (I grupas konkrētais gatavības līmenis = (2 +4) / 2).

Katras grupas vispārējo aptvēruma pakāpi aprēķina kā attiecību starp attiecīgās grupas jautājumu kopskaitu un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši.

Katras grupas konkrēto aptvēruma pakāpi aprēķina kā attiecību starp to grupas jautājumu kopskaitu, kuri attiecas uz mērķiem, ko dalībvalsts ir izvēlējusies novērtēt (tie parasti ir konkrētās valsts VKS ietvertie mērķi), un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši.

Kopējie vērtējumi

Valsts kopējo vispārējo gatavības līmeni aprēķina kā visu sistēmā ietverto mērķu (no 1 līdz 17) gatavības līmeņa aritmētisko vidējo.

Valsts kopējo konkrēto gatavības līmeni aprēķina kā to sistēmas mērķu gatavības līmeņa aritmētisko vidējo, kurus dalībvalsts ir izvēlējusies novērtēt (parasti tie ir konkrētās valsts VKS ietvertie mērķi).

Valsts kopējo vispārējo aptvēruma pakāpi aprēķina kā attiecību starp visu sistēmas mērķu (no 1 līdz 17) jautājumu kopskaitu un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši.

Valsts kopējo konkrēto aptvēruma pakāpi aprēķina kā attiecību starp to jautājumu kopskaitu, kuri attiecas uz sistēmā iekļautajiem mērķiem, ko dalībvalsts ir izvēlējusies novērtēt (tie parasti ir konkrētās valsts VKS ietvertie mērķi), un to jautājumu skaitu, uz kuriem atbildēts apstiprinoši.

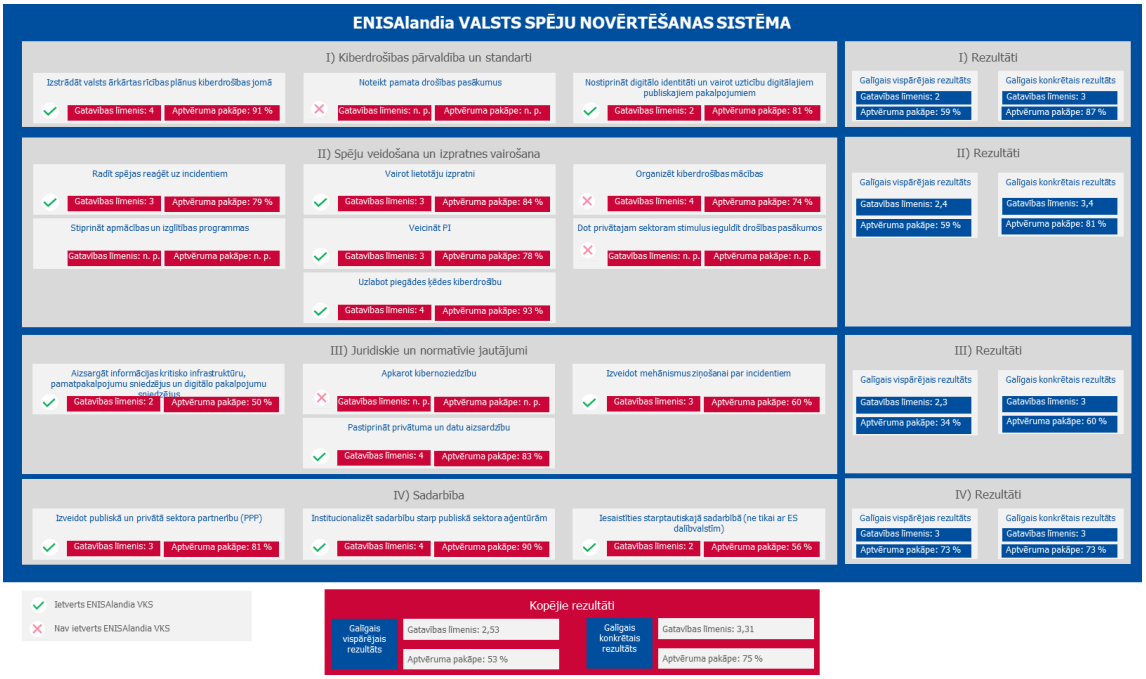
Katram rādītājam respondenti var izvēlēties trešo atbildes variantu "nezinu / nav piemērojams". Šajā gadījumā attiecīgo rādītāju neietver rezultātu kopējā aprēķinā.

Gatavības līmeņus katrai grupai un kopumā aprēķina kā aritmētisko vidējo, lai parādītu izmaiņas starp diviem novērtējumiem. Alternatīva būtu grupas un kopējo gatavības līmeņu aprēķinos pieņemt, ka gatavības līmenis atbilst vismazāk gatavā mērķa līmenim, bet, kaut arī tas sniedz būtisku informāciju par gatavību, tas neatspoguļo panākumus, kas gūti citos mērķos ietvertās jomās.

Tā kā pārskatu vajadzībām grupas un kopējais līmenis ir konsolidēti, tika nolemts izmantot aritmētisko vidējo. Lai pārskatos atspoguļotu precīzāku informāciju, izmantojiet mērķa līmeņa vērtējumus.

3. attēlā tālāk tekstā ir sniegts kopsavilkums par vērtējuma piešķiršanas mehānismiem dažādajos modeļa līmeņos (mērķa, grupas, kopējais līmenis).

3. attēls. Kopējais vērtējuma piešķiršanas mehānisms



3.5 PAŠNOVĒRTĒŠANAS SISTĒMAI IZVIRZĪTĀS PRASĪBAS

Šajā iedaļā aprakstītā valsts spēju novērtēšanas sistēma ir balstīta uz dalībvalstu norādītajām vajadzībām un veidota atbilstoši šādām prasībām:

- dalībvalsts VSNS izmanto brīvprātīgi kā pašnovērtēšanas sistēmu;
- VSNS mērķis ir novērtēt dalībvalstu kiberdrošības spējas attiecībā uz 17 mērķiem; tomēr dalībvalsts var izvēlēties, attiecībā uz kuriem mērķiem veikt novērtējumu, un novērtēt tikai daļu no 17 mērķiem;
- pašnovērtēšanas sistēmas mērķis ir novērtēt dalībvalsts kiberdrošības spēju gatavības līmeni;
- novērtējuma rezultātus publicē tikai tad, ja dalībvalsts pati tā nolemj darīt;
- dalībvalsts var attēlot novērtējuma rezultātus, norādot valsts kiberdrošības spēju, mērķu grupas vai pat tikai atsevišķa mērķa gatavības līmeni;
- visi novērtētie mērķi novērtēšanas sistēmā ir vienlīdz svarīgi, tāpēc tiem ir vienāda nozīme; tas pats attiecas uz sistēmā izmantotajiem rādītājiem;
- dalībvalsts var sekot līdzi progresam laika gaitā.

Pašnovērtēšanas sistēmas mērķis ir palīdzēt dalībvalstīm veidot kiberdrošības spējas, tāpēc tajā ir ietverti arī vairāki ieteikumi vai pamatnostādnes, kas palīdzēs Eiropas valstīm paaugstināt savu gatavības līmeni.

Piezīme: šie ieteikumi vai pamatnostādnes ir vispārīgi un balstīti uz *ENISA* publikācijām un no citām valstīm apkopotām atziņām, un būs atkarīgi no pašnovērtējuma rezultāta.

4. VSNS RĀDĪTĀJI

4.1 SISTĒMAS RĀDĪTĀJI

Šajā iedaļā ir aprakstīti *ENISA* valsts spēju novērtēšanas sistēmas rādītāji. Nākamās iedaļas ir veltītas katra savai grupai.

Katrai grupai tabulā ir iekļauti visi rādītāji kā jautājumi, kas atspoguļo konkrētu gatavības līmeni. Šī anketa ir galvenais pašnovērtēšanas rīks. Katram mērķim ir divi rādītāju kopumi:

- vispārīgi jautājumi par stratēģijas gatavību (9 vispārīgi jautājumi), kas katrā gatavības līmenī atzīmēti ar a–c un atkārtojas katrā mērķī;
- jautājumi par kiberdrošības spējām (319 jautājumi par kiberdrošības spējām), kas sanumurēti no 1 līdz 10 katrā gatavības līmenī un attiecas uz konkrēto mērķa jomu.

Katrs jautājums ir atzīmēts ar 0 vai 1, kas norāda, vai jautājums konkrētajā gatavības līmenī ir obligāts rādītājs (1) vai neobligāts rādītājs (0).

Katru jautājumu var identificēt pēc identifikācijas numura, kas sastāv no:

- mērķa numura,
- gatavības līmeņa un
- jautājuma numura.

Piemēram, jautājums ar identifikācijas numuru 1.2.4 ir pirmā stratēģiskā mērķa “Izstrādāt valsts ārkārtas rīcības plānus kiberdrošības jomā” otrā gatavības līmeņa ceturtais jautājums.

Jāņem vērā, ka visi anketā ietvertie jautājumi attiecas uz valsts līmeni, ja vien nav norādīts citādi. Visos jautājumos vietniekvārds “jūs” attiecas uz dalībvalsti kopumā, nevis uz konkrēto personu vai valdības struktūru, kas veic novērtējumu.

Visu mērķu definīcijas ir sniegtas 2.2. iedaļā “Eiropas VKS konstatētie kopīgie mērķi”.

4.1.1 1. grupa: kiberdrošības pārvaldība un standarti

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
1 – Izstrādāt valsts ārkārtas rīcības plānus kiberdrošības jomā	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķirums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat sākuši strādāt pie valsts ārkārtas rīcības plānu veidošanas kiberdrošības jomā, piem., pie ārkārtas rīcības plānu vispārīgo mērķu, tvēruma un/vai principu noteikšanas?	1	Vai jums ir doktrīna / valsts stratēģija, kurā ir iekļauta kiberdrošība kā krīzes faktors (t. i., plāns, politika utt.)?	1	Vai jums valsts līmenī ir kiberkrīzes pārvarēšanas plāns?	1	Vai esat apmierināti ar to, cik daudz kritisko sektoru pēc skaita vai īpatsvara ir iekļauts valsts ārkārtas rīcības plānā kiberdrošības jomā?	1	Vai jums ir paredzēts process, kā mācīties no pieredzes pēc kiberdrošības mācībām vai reālām krīzēm valsts līmenī?	1
	2	Vai ir vispārpieņemts, ka kiberincidenti ir krīzes faktors, kas var apdraudēt valsts drošību?	0	Vai jums ir kāds centrs, no kura gūt informāciju un ar kura starpniecību informēt lēmumu pieņēmējus, proti, kādas metodes, platformas vai vietas, kas nodrošina, ka visi dalībnieki, kuri ir iesaistīti reaģēšanā uz krīzi, var piekļūt vienai un tai pašai reāllaika informācijai par kiberkrīzi?	1	Vai jums ir valsts procedūras, kas attiecas tieši uz kiberkrīzi?	1	Vai jūs pietiekami bieži organizējat pasākumus (t. i., mācības), kas saistīti ar ārkārtas situāciju plānošanu kiberkrīzes jomā valsts mērogā?	1	Vai jums ir kāds process regulārai valsts plāna izmēģināšanai?	1
	3	Vai ir veikti pētījumi (tehniski, darbības, politiski) attiecībā uz ārkārtas situāciju plānošanu kiberdrošības jomā?	0	Vai ir iesaistīti atbilstošie resursi, kas nepieciešami, lai pārraudzītu, kā tiek izstrādāti un izpildīti valsts ārkārtas rīcības plāni kiberdrošības jomā?	1	Vai jums ir komunikācijas grupa, kas ir īpaši apmācīta reaģēt uz kiberkrīzēm un informēt sabiedrību?	1	Vai jums ir pietiekami daudz cilvēku, kas nodarbojas ar krīžu plānošanu, gūto mācību izskatīšanu un pārmaiņu ieviešanu?	1	Vai jums ir atbilstoši rīki un platformas, kas palīdz apzināties situāciju?	1
	4	-		Vai jums valsts līmenī ir kiberdraudu novērtēšanas metodika, kas ietver ietekmes novērtēšanas procedūras?	0	Vai jūs iesaistāt visas attiecīgās valsts ieinteresētās personas (valsts drošības, aizsardzības, civilās aizsardzības, tiesībaizsardzības pārstāvjus, ministrijas, iestādes utt.)?	1	Vai jums ir pietiekami daudz cilvēku, kas ir apmācīti reaģēt uz kiberkrīzēm valsts līmenī?	1	Vai jūs izmantojat īpašu gatavības modeli, lai uzraudzītu un uzlabotu ārkārtas rīcības plānu kiberdrošības jomā?	0
	5	-		-		Vai jums ir pienācīgi krīzes pārvaldības objekti un dežūrpunkti?	1	-		Vai jums ir tādi resursi, kas ir specializējušies apdraudējumu prognozēšanā vai arī strādā prognostiskās kiberdrošības jomā, lai novērstu turpmākas krīzes vai stātos pretī nākotnes izaicinājumiem?	0
	6	-		-		Vai jūs nepieciešamības gadījumā sadarbojaties ar starptautiskām ieinteresētajām personām ES?	0	-		-	
	7	-		-		Vai jūs nepieciešamības gadījumā sadarbojaties ar starptautiskām ieinteresētajām personām trešās valstīs?	0	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
2 – Noteikt pamata drošības pasākumus	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumu, lai noteiktu prasības un nepilnības **publiskā sektora** organizācijām, pamatojoties uz starptautiski atzītiem standartiem, piem., ISO27001, ISO27002, BS 15000, EN ISO27799, *PCI-DSS*, *CobiT*, *ITIL*, *BSI IT-Grundschutz*, *IETF*, *IEEE*, *NIST*, *FIPS*, *ITU*, *ISA*, *IEC*, *CIS*?	1	Vai drošības pasākumi ir izstrādāti saskaņā ar starptautiskiem/valsts standartiem?	1	Vai pamata drošības pasākumi ir obligāti?	1	Vai ir noteikts process, kā regulāri atjaunināt pamata drošības pasākumus?	1	Vai jums ir noteikts process, kā stiprināt IKT gadījumos, kad incidentus neizdodas novērst ar šiem pasākumiem?	1
	2	Vai jūs esat veikuši pētījumu, lai noteiktu prasības un nepilnības **privātā sektora** organizācijām, pamatojoties uz starptautiski atzītiem standartiem, piem., ISO27001, ISO27002, BS 15000, EN ISO27799, *PCI-DSS*, *CobiT*, *ITIL*, *BSI IT-Grundschutz*, *IETF*, *IEEE*, *NIST*, *FIPS*, *ITU*, *ISA*, *IEC*, *CIS*?	1	Vai, nosakot pamata drošības pasākumus, tiek uzklausīts privātais sektors un citas ieinteresētās personas?	1	Vai jūs īstenojat horizontālus drošības pasākumus visās kritiskajās nozarēs?	1	Vai ir ieviests uzraudzības mehānisms, ar ko var noskaidrot, cik lielā mērā tiek īstenoti pamata drošības pasākumi?	1	Vai jūs izvērtējat, cik atbilstoši ir jauni standarti, kas tiek izstrādāti, reaģējot uz jaunākajām apdraudējumu ainas izmaiņām?	1
	3	-		-		Vai jūs īstenojat nozaru drošības pasākumus visās kritiskajās nozarēs?	1	Vai kādai valsts iestādei ir uzdevums pārbaudīt, vai pamata drošības pasākumi tiek veikti vai ne?	1	Vai jums ir koordinētas ievainojamību atklāšanas (*CVD*) valsts process, vai arī jūs tādu veicināt?	1
	4	-				Vai pamata drošības pasākumi atbilst attiecīgām sertifikācijas shēmām?	1	Vai jums ir ieviests process, kā noteiktā laikposmā atklāt neatbilstīgas organizācijas?	1	-	
	5	-		-		Vai pamata drošības pasākumiem ir ieviests riska pašnovērtēšanas process?	1	Vai ir ieviests revīzijas process, lai pārliecinātos, vai drošības pasākumi tiek piemēroti pareizi?	1	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	R
2 – Noteikt pamata drošības pasākumus	6	-		-		Vai jūs pārskatāt obligātos pamata drošības pasākumus valdības struktūru iepirkuma procesā?	0	Vai jūs nosakāt drošus standartus kritisko IT/OT produktu (medicīniskā aprīkojuma, satīklotu un autonomu transportlīdzekļu, profesionāla radioaprīkojuma, smagās rūpniecības aprīkojuma utt.) izstrādei vai aktīvi veicināt šādu standartu pieņemšanu?	0	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
3 – Nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķirums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumus vai nepilnību analīzes, lai noteiktu vajadzības, kas saistītas ar iedzīvotājiem un uzņēmumiem sniegto digitālo publisko pakalpojumu drošības panākšanu?	1	Vai jūs veicat riska analīzes, lai noteiktu līdzekļu vai pakalpojumu riska profilu, pirms tos pārvietojat uz mākoni vai sākat digitālās pārveides projektus?	1	Vai jūs sekmējat integrētās privātuma aizsardzības metodiku izmantošanu visos e-pārvaldes projektos?	1	Vai jūs apkopojat rādītājus par kiberdrošības incidentiem, kuru ietvaros ir pārkāpta digitālo publisko pakalpojumu drošība?	1	Vai jūs piedalāties Eiropas darba grupās, lai uzturētu standartus un/vai izstrādātu jaunas prasības elektroniskajiem uzticamības pakalpojumiem (e-parakstiem, e-zīmogiem, elektroniskajiem piegādes pakalpojumiem, laika zīmogošanai, tīmekļa vietņu autentifikācijai), piem., *ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU*?	1
	2	-		Vai jums ir stratēģija, kā veidot vai veicināt drošas valsts elektroniskās identifikācijas shēmas (e-ID) iedzīvotājiem un uzņēmumiem?	1	Vai jūs iesaistāt privātā sektora ieinteresētās personas drošu digitālo publisko pakalpojumu izstrādē un nodrošināšanā?	1	Vai jūs un citas dalībvalstis savstarpēji atzīstat cita citas e-identifikācijas līdzekļus?	1	Vai jūs aktīvi piedalāties salīdzinošajā izvērtēšanā, kas tiek veikta saistībā ar e-ID shēmu paziņošanu Eiropas Komisijai?	1
	3	-		Vai jums ir stratēģija, kā veidot vai veicināt drošus valsts elektroniskos uzticamības pakalpojumus (e-parakstus, e-zīmogus, elektroniskos piegādes pakalpojumus, laika zīmogošanu, tīmekļa vietņu autentifikāciju) iedzīvotājiem un uzņēmumiem?	1	Vai jūs ievērojat minimālos drošības principus visos digitālajos publiskajos pakalpojumos?	1	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
3 – Nostiprināt digitālo identitāti un vairot uzticību digitālajiem publiskajiem pakalpojumiem	4	-		Vai jums ir valdības mākoņa stratēģija (mākoņdatošanas stratēģija, kura paredzēta valdībai un publiskā sektora struktūrām, piemēram, ministrijām, valdības aģentūrām un valsts pārvaldes iestādēm), kurā ir ņemti vērā drošības apsvērumi?	0	Vai iedzīvotājiem un uzņēmumiem ir pieejamas kādas elektroniskās identifikācijas shēmas, kurām ir būtisks vai augsts uzticamības līmenis, kā noteikts *eIDAS* regulas (Regula (ES) Nr. 910/2014) pielikumā?	1	-		-	
	5	-		-		Vai jums ir digitāli publiskie pakalpojumi, kam ir vajadzīgas elektroniskās identifikācijas shēmas, kurām ir būtisks vai augsts uzticamības līmenis, kā noteikts *eIDAS* regulas (Regula (ES) Nr. 910/2014) pielikumā?	1	-		-	
	6	-		-		Vai jums ir iedzīvotājiem un uzņēmumiem pieejami uzticamības pakalpojumu sniedzēji (e-paraksti, e-zīmogi, elektroniskie piegādes pakalpojumi, laika zīmogošana, tīmekļa vietņu autentifikācija)?	1	-		-	
	7	-		-		Vai jūs veicināt pamata drošības pasākumu pieņemšanu visos mākoņa izvietošanas modeļos (piem., privātajos, publiskajos, hibrīda, infrastruktūrā kā pakalpojumā, platformā kā pakalpojumā, programmatūrā kā pakalpojumā)?	0	-		-	

4.1.2 2. grupa: spēju veidošana un izpratnes vairošana

VKS mērķis	Nr.	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
4 – Radīt spējas reaģēt uz incidentiem	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jums ir neformālas spējas reaģēt uz incidentiem, kuras tiek pārvaldītas publiskajā un privātajā sektorā vai to starpā?	1	Vai jums ir vismaz viena oficiāla valsts datordrošības incidentu reaģēšanas vienība (*CSIRT*)?	1	Vai jums ir spējas reaģēt uz incidentiem TID direktīvas II pielikumā minētajās nozarēs?	1	Vai jūs esat noteikuši un veicinājuši standartizētu praksi attiecībā uz reaģēšanas uz incidentiem procedūrām un incidentu klasifikācijas shēmām?	1	Vai jums ir mehānismi nulles dienas ievainojamību agrīnai atklāšanai, identificēšanai, novēršanai, reaģēšanai uz tām un to ietekmes mazināšanai?	1
	2	-		Vai jūsu valsts *CSIRT* ir skaidri noteikts iejaukšanās tvērums, piem., atkarībā no mērķa nozares, incidenta veidiem, ietekmes?	1	Vai jūsu valstī ir *CSIRT* sadarbības mehānisms reaģēšanai uz incidentiem?	1	Vai jūs izvērtējat savas spējas reaģēt uz incidentiem, lai pārliecinātos, ka jums ir pienācīgi resursi un prasmes TID direktīvas I pielikuma 2. punktā izklāstīto uzdevumu veikšanai?	1	-	
	3	-		Vai jūsu valsts *CSIRT* ir skaidri noteiktas attiecības ar citām valsts ieinteresētajām personām (piem., tiesībaizsardzības iestādēm, militārpersonām, interneta pakalpojumu sniedzējiem, nacionālo kiberdrošības centru) attiecībā uz valsts kiberdrošības ainu un reaģēšanā uz incidentiem izmantoto praksi?	0	Vai jūsu valsts *CSIRT* ir TID direktīvas I pielikumā paredzētās spējas reaģēt uz incidentiem, t. i., spējas nodrošināt pieejamību, fizisko drošību, darbības nepārtrauktību, starptautisko sadarbību, incidentu uzraudzību, brīdināšanu un agrīno brīdināšanu, reaģēt uz incidentu, nodrošināt risku analīzi un situācijas apzināšanos, sadarboties ar privāto sektoru, standarta prakse utt.?	1	-		-	
	4	-				Vai ir mehānisms sadarbībai ar kaimiņvalstīm saistībā ar incidentiem?	1	-		-	
	5	-		-		Vai jūs esat oficiāli noteikuši skaidru politiku un procedūras rīcībai incidentu gadījumā?	1	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
4 – Radīt spējas reaģēt uz incidentiem	6	-		-		Vai jūsu valsts *CSIRT* piedalās kiberdrošības mācībās gan valsts, gan starptautiskā līmenī?	1	-		-	
	7	-		-		Vai jūsu valsts *CSIRT* piedalās *FIRST* (Incidentu reaģēšanas un drošības vienību forumā)?	0	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
5 – Vairot lietotāju izpratni	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai valdība, privātais sektors vai parastie lietotāji kaut nedaudz atzīst, ka ir jāpalielina informētība par kiberdrošības un privātuma jautājumiem?	1	Vai jūs esat noteikuši konkrētu mērķauditoriju lietotāju izpratnes vairošanas centieniem, piem., parastie lietotāji, jaunieši, komerclietotāji (ko var iedalīt sīkāk MVU, pamatpakalpojumu sniedzējos, digitālo pakalpojumu sniedzējos utt.)?	1	Vai jūs esat izstrādājuši komunikācijas plānus/stratēģiju kampaņām?	1	Vai jūs izstrādājat kampaņas izvērtēšanas rādītājus plānošanas posmā?	1	Vai jums ir ieviesti mehānismi, kas nodrošina, ka izpratnes vairošanas kampaņās pastāvīgi tiek sniegta aktuāla informācija, ņemot vērā tehnoloģiju attīstību, pārmaiņas apdraudējumu ainā, normatīvo regulējumu un valsts priekšrakstus drošības jomā?	1
	2	Vai publiskā sektora aģentūras īsteno kiberjautājumu izpratnes vairošanas kampaņas savā organizācijā pēc nepieciešamības, piem., pēc kiberdrošības incidenta?	0	Vai jūs sagatavojat projekta plānu, saskaņā ar kuru vairot izpratni par informācijas drošības un privātuma jautājumiem?	1	Vai jums ir satura veidošanas process valdības līmenī?	1	Vai jūs izvērtējat savas kampaņas pēc to īstenošanas?	1	Vai jūs periodiski veicat izvērtējumus vai pētījumus, lai privātajā un publiskajā sektorā apzinātu izmaiņas attieksmē vai uzvedībā kiberdrošības un privātuma jautājumos?	1

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
5 – Vairot lietotāju izpratni	3	Vai publiskā sektora aģentūras īsteno plašai sabiedrībai paredzētas kiberjautājumu izpratnes vairošanas kampaņas pēc vajadzības, piem., pēc kiberdrošības incidenta?	0	Vai jums ir pieejami un viegli atrodami resursi (piem., vienots tiešsaistes portāls, izpratnes veicināšanas komplekti), ko ikviens lietotājs var izmantot, lai gūtu informāciju par kiberdrošības un privātuma jautājumiem?	1	Vai jums ir mehānismi, ar ko noteikt jomas, kurās būtu jāvairo izpratne (piem., *ENISA* apdraudējumu aina, valstu ainas, starptautiskās ainas, atsauksmes no valsts kibernoziedzības apkarošanas centriem)?	1	Vai jums ir ieviesti mehānismi, ar ko noteikt vissvarīgākos plašsaziņas līdzekļus vai komunikācijas kanālus, kuri dotu vislabākās iespējas maksimāli sasniegt un iesaistīt konkrēto mērķauditoriju (piem., dažādu veidu digitālie plašsaziņas līdzekļi, brošūras, e-pasts, mācību materiāli, plakāti vietās, kur uzturas daudz cilvēku, televīzija, radio)?	1	Vai jūs apspriežaties ar uzvedības ekspertiem, lai pielāgotu savu kampaņu konkrētai mērķauditorijai?	1
	4	-		-		Vai jūs satura radīšanā iesaistāt gan ieinteresētās personas, gan arī ekspertus un komunikācijas komandas, kuri savā starpā sadarbojas?	1			-	
	5	-		-		Vai jūs savos izpratnes vairošanas centienos iesaistāt un ieinteresējat privāto sektoru, lai popularizētu vēstījumus un tos izplatītu plašākai auditorijai?	1	-		-	
	6	-		-		Vai jūs sagatavojat īpašas izpratnes vairošanas iniciatīvas vadošajiem darbiniekiem publiskajā, privātajā, akadēmiskajā vai pilsoniskās sabiedrības sektorā?	1	-		-	
	7	-		-		Vai jūs piedalāties *ENISA* Eiropas kiberdrošības mēneša (*ECSM*) kampaņās?	0	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
6 – Organizēt kiberdrošības mācības	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
6 – Organizēt kiberdrošības mācības	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs vadāt krīzes mācības citās nozarēs (ne kiberdrošības jomā) valsts vai Eiropas līmenī?	1	Vai jums ir valsts līmeņa kiberdrošības mācību programma?	1	Vai jūs iesaistāt visas attiecīgās valsts pārvaldes iestādes (pat ja scenārijs attiecas uz konkrētu nozari)?	1	Vai jūs sagatavojat ziņojumus par uzdevuma izpildes rezultātiem / izvērtējuma ziņojumus?	1	Vai jums ir iespējas analizēt gūtās mācības kiberdrošības jomā (ziņošanas procesi, analīze, ietekmes mazināšana)?	1
	2	Vai jūs esat piešķīruši resursus krīzes pārvarēšanas mācību izstrādei un plānošanai?	1	Vai jūs īstenojat vai nosakāt par prioritāti krīzes pārvarēšanas mācības svarīgu sabiedrisko funkciju un kritiskās infrastruktūras jomā?	1	Vai jūs iesaistāt privāto sektoru mācību plānošanā un īstenošanā?	1	Vai jūs izmēģināt valsts līmeņa plānus un procedūras?	1	Vai jums ir iedibināts process, kā mācīties no pieredzes?	1
	3	-		Vai jūs esat noteikuši koordinācijas struktūru (publiskā sektora aģentūru, konsultāciju uzņēmumu utt.), kas pārrauga kiberdrošības mācību izstrādi un plānošanu?	0	Vai jūs organizējat nozares mācības valsts un/vai starptautiskā mērogā?	1	Vai jūs piedalāties Eiropas mēroga kiberdrošības mācībās?	1	Vai jūs pielāgojat mācību scenārijus atbilstoši jaunākajiem pavērsieniem (tehnoloģiju attīstība, konflikti pasaulē, apdraudējumu aina utt.)?	1
	4	-		-		Vai jūs organizējat mācības visās kritiskajās nozarēs, kas minētas TID direktīvas II pielikumā?	1	-		Vai jūs saskaņojat savas krīžu pārvarēšanas procedūras ar citām dalībvalstīm, lai nodrošinātu efektīvu krīzes pārvarēšanu Eiropas mērogā?	1
	5	-		-		Vai jūs organizējat nozares un/vai starpnozaru kiberdrošības mācības?	1	-		Vai jums ir ieviests mehānisms, kā ātri pielāgot stratēģiju, plānus un procedūras, ņemot vērā mācībās gūto pieredzi?	0
	6	-		-		Vai jūs organizējat kiberdrošības mācības, kas attiecas uz konkrētu līmeni (tehnisko un darbības līmeni, procedūru līmeni, lēmumu pieņemšanas līmeni, politisko līmeni utt.)?	0	-		-	

VKS mērķis	#	Level 1	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
7 – Stiprināt apmācības un izglītības programmas	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs apsverat iespēju izstrādāt kiberdrošības apmācības un izglītības programmas?	1	Vai jūs veidojat kiberdrošībai veltītus kursus?	1	Vai jūsu valstī kiberdrošības kultūras jautājumi tiek ietverti jau agrīnā studentu izglītības ceļa posmā? Piemēram, vai jūs pievēršat uzmanību kiberdrošībai pamatizglītības otrajā posmā un vidusskolā?	1	Vai jūs mudināt privātā un publiskā sektora darbiniekus tikt akreditētiem vai sertificētiem?	1	Vai jums ir ieviesti mehānismi, kas nodrošina, ka apmācībās un izglītības programmās pastāvīgi tiek sniegta aktuāla informācija, ņemot vērā pašreizējās un jaunās tendences tehnoloģiju attīstībā, pārmaiņas apdraudējumu ainā, normatīvo regulējumu un valsts priekšrakstus drošības jomā?	1
	2	-		Vai jūsu valsts universitātēs ir iespējams iegūt doktora grādu kiberdrošības jomā kā atsevišķā disciplīnā, nevis kā vienā no priekšmetiem datorzinātņu programmā?	1	Vai jums ir valsts pētniecības laboratorijas un izglītības iestādes, kas ir specializējušās kiberdrošības jomā?	1	Vai jūsu valsts ir izstrādājusi kiberdrošības apmācības vai mentorēšanas programmas, lai atbalstītu valsts jaunuzņēmumus un MVU?	1	Vai jūs dibināt akadēmiskos kiberdrošības izcilības centrus, kas darbojas kā pētniecības un izglītības centri?	1
	3	-		Vai jūs plānojat apmācīt pedagogus par informācijas drošības un privātuma jautājumiem (piem., drošību internetā, persondatu aizsardzību, iebiedēšanu tiešsaistē) neatkarīgi no viņu darbības jomas?	1	Vai jūs veicināt/finansējat speciālus kiberdrošības kursus un apmācības plānus dalībvalsts nodarbinātības aģentūru darbiniekiem?	1	Vai jūs aktīvi veicināt informācijas drošības kursu iekļaušanu augstākajā izglītībā ne tikai informātikā, bet arī citās profesionālajās specialitātēs, piem., tādu informācijas drošības kursu iekļaušanu, kuri ir pielāgoti konkrētās profesijas vajadzībām?	1	Vai akadēmiskās iestādes piedalās diskusiju par kiberdrošības izglītību un pētniecību vadīšanā starptautiskā mērogā?	0
	4	-		-		Vai jums ir kiberdrošības kursi un/vai speciāla mācību programma Eiropas kvalifikāciju ietvarstruktūras 5.–8. līmenim?	1	Vai jūs regulāri novērtējat prasmju nepietiekamību (kiberdrošības jomas darbinieku trūkumu) informācijas drošības jomā?	1	-	
	5	-		-		Vai jūs veicināt un/vai atbalstāt iniciatīvas iekļaut interneta drošības kursus pamata un vidējā izglītībā?	1	Vai jūs veicināt tīklošanos un dalīšanos ar informāciju starp akadēmiskajām iestādēm gan valsts, gan starptautiskā līmenī?	1		

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
7 - Stiprināt apmācības un izglītības programmas	6	-		-		Vai jūs finansējat vai piedāvājat bez maksas pamata kiberdrošības apmācību iedzīvotājiem?	0	Vai jūs iesaistāt privāto sektoru jebkādās kiberdrošības izglītības iniciatīvās (piem., kursu izstrāde un nodrošināšana, stažēšanās, prakse)?	1	-	
	7	-		-		Vai jūs organizējat ikgadējus informācijas drošības pasākumus (piem., programmēšanas sacensības jeb hakatonus)?	0	Vai jūs izmantojat finansēšanas mehānismus, lai veicinātu augstākās izglītības ieguvi kiberdrošības jomā, piem., stipendijas, garantētas mācekļa/prakses vietas, garantētu darbu konkrētā nozarē vai amatus publiskajā sektorā?	0	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
8 – Veicināt PI	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumus vai analīzes, lai noteiktu pētniecības un izstrādes prioritātes kiberdrošības jomā?	1	Vai jums ir process pētniecības un izstrādes prioritāšu noteikšanai (piem., jauni jautājumi, kas saistīti ar atturēšanu no jaunu veidu kiberuzbrukumiem, aizsardzību pret tiem, to atklāšanu un pielāgošanos tiem)?	1	Vai jūs plānojat sasaistīt pētniecības un izstrādes iniciatīvas ar reālo ekonomiku?	1	Vai kiberdrošības pētniecības un izstrādes iniciatīvas atbilst attiecīgiem stratēģiskajiem mērķiem, piem., tiem, kas saistīti ar digitālo vienoto tirgu, programmu “Apvārsnis 2020”, programmu “Digitālā Eiropa”, ES kiberdrošības stratēģiju?	1	Vai jūs valsts līmenī sadarbojaties ar starptautiskām pētniecības un izstrādes iniciatīvām, kas saistītas ar kiberdrošību?	1
	2	-		Vai privātais sektors ir iesaistīts pētniecības un izstrādes prioritāšu noteikšanā?	1	Vai ir izveidoti ar kiberdrošību saistīti valsts projekti?	1	Vai ir ieviesta pētniecības un izstrādes iniciatīvu izvērtēšanas shēma?	1	Vai pētniecības un izstrādes prioritātes saskan ar pašreizējo vai gaidāmo valsts līmeņa regulējumu?	1

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
8 – Veicināt PI	3	-		Vai akadēmiskās aprindas ir iesaistītas pētniecības un izstrādes prioritāšu noteikšanā?	1	Vai jums ir vietējas/reģionālas jaunuzņēmumu ekosistēmas un citi tīklošanās kanāli (piem., tehnoloģiju parki, inovācijas kopas, tīklošanās pasākumi/platformas), kas veicina inovāciju (tostarp kiberdrošības jaunuzņēmumos)?	1	Vai ir noslēgti sadarbības nolīgumi ar universitātēm un citām pētniecības iestādēm?	1	Vai jūs piedalāties starptautiska līmeņa diskusiju vadīšanā par vienu vai daudziem progresīvas pētniecības un izstrādes jautājumiem?	0
	4	-		Vai kādas valsts pētniecības un izstrādes iniciatīvas ir saistītas ar kiberdrošību?	0	Vai tiek veikti ieguldījumi kiberdrošības pētniecības un izstrādes programmās akadēmiskajā un privātajā sektorā?	1	Vai ir kāda atzīta institucionāla struktūra, kas pārrauga kiberdrošības pētniecības un izstrādes darbības?	0	-	
	5	-		-		Vai jūsu universitātēs ir rūpnieciskās pētniecības katedru vadītāji, kas var palīdzēt sasaistīt pētniecības tematus ar tirgus vajadzībām?	1	-		-	
	6	-		-		Vai jums ir īpašas pētniecības un izstrādes finansēšanas programmas kiberdrošības jomā?	0	-		-	

VKS mērķis	#	Level 1	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
9— Dot privātajam sektoram stimulus ieguldīt drošības pasākumos	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai ir nozares politika, kas veicina kiberdrošības nozares attīstību, vai politiska griba to veicināt?	1	Vai privātais sektors ir iesaistīts stimulu radīšanā?	1	Vai ir radīti ekonomiski/regulatīvi vai citu veidu stimuli, kas veicina ieguldījumus kiberdrošības jomā?	1	Vai kādi privātā sektora dalībnieki ir reaģējuši uz stimuliem ar ieguldījumiem drošības pasākumos, piem., kiberdrošībā specializējušies ieguldītāji un ieguldītāji, kam šādas specializācijas nav?	1	Vai jūs kiberdrošības jautājumus, uz kuriem vērst stimulus, izvēlaties atkarībā no jaunākajām izmaiņām apdraudējumu jomā?	1

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
9— Dot privātajam sektoram stimulus ieguldīt drošības pasākumos	2	-		Vai jūs esat noteikuši, kuri kiberdrošības aspekti būtu jāpilnveido (piem., kriptogrāfija, privātums, jauni autentifikācijas veidi, kiberdrošības mākslīgais intelekts)?	0	Vai jūs sniedzat atbalstu (piem., nodokļu stimulus) kiberdrošības jaunuzņēmumiem un MVU?	1	Vai jūs stimulējat privāto sektoru pievērsties augsto tehnoloģiju, piem., 5G, mākslīgā intelekta, lietu interneta, kvantiskās datošanas, drošībai?	1	-	
	3	-		-		Vai jūs ar nodokļu stimuliem vai kādu citu finansiālu motivāciju mudināt privātā sektora ieguldītājus investēt kiberdrošības jaunuzņēmumos?	1	-		-	
	4	-		-		Vai jūs atvieglojat kiberdrošības jaunuzņēmumu un MVU iespējas piedalīties publiskā iepirkuma procesā?	0	-		-	
	5	-		-		Vai ir pieejams budžets, ko var izmantot, lai sniegtu stimulus privātajam sektoram?	0	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
10 – Uzlabot piegādes ķēdes kiberdrošību	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumu par dažādos nozares segmentos un/vai publiskajā sektorā iepirkumos izmantotu labu drošības praksi piegādes ķēdes pārvaldībā?	1	Vai jūs vērtējat kiberdrošību visā IKT pakalpojumu un produktu piegādes ķēdē kritiskajās nozarēs (kuras norādītas TID direktīvas (Direktīva (ES) 2016/1148) II pielikumā)?	1	Vai jūs izmantojat drošības sertifikācijas shēmu IKT produktiem un pakalpojumiem, piem., *SOG-IS MRA* (Augstāko amatpersonu grupa informācijas sistēmu drošības savstarpējās atzīšanas nolīguma jautājumos) Eiropā, Vienošanos par kopējo kritēriju atzīšanu (*CCRA*), valsts iniciatīvas, nozaru iniciatīvas?	1	Vai jums ir ieviests process, kā atjaunināt IKT pakalpojumu un produktu piegādes ķēdes kiberdrošības novērtējumus kritiskajās nozarēs (kuras norādītas TID direktīvas (Direktīva (ES) 2016/1148) II pielikumā)?	1	Vai jums piegādes ķēdes svarīgākajos elementos ir ieviestas atklāšanas zondes, lai atklātu agrīnas kompromitējuma pazīmes, piem., interneta pakalpojumu sniedzēja drošības kontroles, drošības zondes būtiskos infrastruktūras komponentos?	1

VKS mērķis	Nr.	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
10 – Uzlabot piegādes ķēdes kiberdrošību	2	-		Vai jūs valsts pārvaldes iepirkuma politikā piemērojat standartus, piem., ISO/IEC 27001 un 27002, ISO/IEC 27036, lai nodrošinātu, ka IKT produktu vai pakalpojumu sniedzēji ievēro pamata informācijas drošības prasības?	1	Vai jūs aktīvi veicināt integrētās drošības un integrētā privātuma paraugprakses izmantošanu IKT produktu un pakalpojumu izstrādē, piem., drošu programmatūras izstrādes dzīves ciklu, lietu interneta dzīves ciklu?	1	Vai jums ir ieviests process, kā noteikt kiberdrošības ziņā vājos piegādes ķēdes posmus kritiskajās nozarēs (kuras norādītas TID direktīvas (Direktīva (ES) 2016/1148) II pielikumā)?	1	-	
	3	-		-		Vai jūs izstrādājat un nodrošināt centralizētus katalogus ar vispusīgu informāciju par pastāvošajiem informācijas drošības un privātuma standartiem, ko var mēroga ziņā pielāgot un piemērot MVU?	1	Vai jums ir ieviesti mehānismi, kas nodrošina, ka pamatpakalpojumu sniedzējiem kritiski svarīgie IKT produkti un pakalpojumi ir noturīgi pret kiberdraudiem (t. i., tie spēj saglabāt pieejamību un drošumu kiberincidenta gadījumā), piem., testēšana, regulāri novērtējumi, kompromitētu elementu atklāšana?	1	-	
	4	-				Vai jūs aktīvi piedalāties ES Kiberdrošības aktā (Regulā (ES) 2019/881) paredzētā IKT digitālo produktu, pakalpojumu un procesu ES sertifikācijas satvara izstrādē, piem., piedalāties Eiropas Kiberdrošības sertifikācijas grupā (*ECCG*), veicināt IKT produktu/pakalpojumu drošības tehniskos standartus un procedūras?	0	Vai jūs veicināt MVU paredzētu sertifikācijas shēmu izstrādi, lai pastiprinātu informācijas drošības un privātuma standarta izmantošanu?	0	-	
	5	-		-		Vai jūs sniedzat MVU kaut kāda veida stimulus, lai mudinātu tos pieņemt drošības un privātuma standartus?	0	Vai jums ir ieviesti kādi pasākumi, kas mudina lielus uzņēmumus uzlabot to piegādes ķēdēs ietilpstošu mazo uzņēmumu kiberdrošību, piem., kiberdrošības centrs, apmācības un izpratnes vairošanas kampaņas?	0	-	
	6	-		-		Vai jūs mudināt programmatūras pārdevējus atbalstīt MVU, nodrošinot drošu noklusējuma konfigurāciju produktos, kas paredzēti mazām organizācijām?	0	-		-	

4.1.3 3. grupa: juridiskie un normatīvie jautājumi

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
11 – Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai valda uzskats, ka informācijas kritiskās infrastruktūras operatori stiprina valsts drošību?	1	Vai jums ir pamatpakalpojumu noteikšanas metodika?	1	Vai jūs esat ieviesuši TID direktīvu (Direktīvu (ES) 2016/1148)?	1	Vai jums ir risku reģistra atjaunināšanas procedūra?	1	Vai jūs sagatavojat un atjaunināt ziņojumus par apdraudējumu ainu?	1
	2	-		Vai jums ir informācijas kritiskās infrastruktūras apzināšanas metodika?	1	Vai jūs esat ieviesuši *ECI* direktīvu (Direktīvu 2008/114/EK) par to, lai apzinātu un noteiktu Eiropas kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību?	1	Vai jums ir ieviesti citi mehānismi, ar ko novērtēt, vai pamatpakalpojumu sniedzēju īstenotie tehniskie un organizatoriskie pasākumi ir pietiekami, lai pārvaldītu tīklu un informācijas sistēmu drošības riskus, piem., regulāras kiberdrošības revīzijas, standarta pasākumu īstenošanas valsts satvars, valdības nodrošināti tehniski rīki, piemēram, atklāšanas zondes vai sistēmas konfigurācijas pārbaude?	1	Vai jums ir iespēja atkarībā no jaunākajām izmaiņām apdraudējumu ainā iekļaut savā informācijas kritiskās infrastruktūras aizsardzības rīcības plānā jaunu nozari?	1
	3	-		Vai jums ir pamatpakalpojumu sniedzēju noteikšanas metodika?	1	Vai jums ir valsts reģistrs, kurā uzskaitīti noteiktie pamatpakalpojumu sniedzēji katrā kritiskajā nozarē?	1	Vai jūs pārskatāt un pēc tam attiecīgi atjaunināt noteikto pamatpakalpojumu sniedzēju sarakstu vismaz ik pēc diviem gadiem?	1	Vai jums ir iespēja atkarībā no jaunākajām izmaiņām apdraudējumu ainā iekļaut savā informācijas kritiskās infrastruktūras aizsardzības rīcības plānā jaunas prasības?	1

VKS mērķis	#											
11 – Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus	4	-		Vai jums ir digitālo pakalpojumu sniedzēju noteikšanas metodika?	1	Vai jums ir valsts reģistrs, kurā uzskaitīti noteiktie digitālo pakalpojumu sniedzēji katrā kritiskajā nozarē?	1	Vai jums ir ieviesti citi mehānismi, ar ko novērtēt, vai digitālo pakalpojumu sniedzēju īstenotie tehniskie un organizatoriskie pasākumi ir pietiekami, lai pārvaldītu tīklu un informācijas sistēmu drošības riskus, piem., regulāras kiberdrošības revīzijas, standarta pasākumu īstenošanas valsts satvars, valdības nodrošināti tehniski rīki, piemēram, atklāšanas zondes vai sistēmas konfigurācijas pārbaude?	1	-	
	5	-		Vai viena vai vairākas no jūsu valsts iestādēm uzrauga informācijas kritiskās infrastruktūras aizsardzību un tīklu un informācijas sistēmu drošību, piem., kā tas ir prasīts TID direktīvā (Direktīvā (ES) 2016/1148)?	1	Vai jums ir valsts risku reģistrs, kurā uzskaitīti atklātie vai zināmie riski?	1	Vai jūs pārskatāt un pēc tam attiecīgi atjaunināt noteikto digitālo pakalpojumu sniedzēju sarakstu vismaz ik pēc diviem gadiem?	1	-	
	6	-		Vai jūs izstrādājat nozaru aizsardzības plānus, piem., tādus, kuros iekļauti pamata kiberdrošības pasākumi (obligāti vai ieteicami)?	0	Vai jums ir informācijas kritiskās infrastruktūras atkarību kartēšanas metodika?	1	Vai jūs izmantojat drošības sertifikācijas shēmu (valsts vai starptautisku), piem., *SOG-IS MRA* Eiropā vai valsts iniciatīvas, lai palīdzētu pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem apzināt drošus IKT produktus?	1	-	
	7	-		-		Vai jūs izmantojat riska pārvaldības praksi, lai apzinātu, kvantitatīvi noteiktu un pārvarētu ar informācijas kritisko infrastruktūru saistītus riskus valsts līmenī?	1	Vai jūs izmantojat drošības sertifikācijas shēmu vai kvalifikācijas procedūru, lai novērtētu pakalpojumu sniedzējus, kas sadarbojas ar pamatpakalpojumu sniedzējiem, piem., pakalpojumu sniedzējus, kas darbojas incidentu atklāšanas, reaģēšanas uz incidentiem, kiberdrošības revīzijas, mākoņpakalpojumu, viedkaršu jomā?	1	-	
	8	-		-		Vai jūs iesaistāties apspriešanās procesā, lai atklātu pārrobežu atkarības?	1	Vai jums ir ieviesti mehānismi, ar ko novērtēt, cik labi pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji īsteno pamata kiberdrošības pasākumus?	0	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
11 – Aizsargāt informācijas kritisko infrastruktūru, pamatpakalpojumu sniedzējus un digitālo pakalpojumu sniedzējus	9					Vai jums ir vienots kontaktpunkts, kura uzdevums ir koordinēt jautājumus, kas saistīti ar tīklu un informācijas sistēmu drošību valsts līmenī un pārrobežu sadarbību Savienības līmenī?	1	Vai jums ir ieviesti kādi mehānismi, kas nodrošina informācijas kritiskās infrastruktūras sniegto pakalpojumu nepārtrauktību, piem., krīžu paredzēšana, kritisko informācijas sistēmu atjaunošanas procedūras, darbības nepārtrauktības nodrošināšana bez IT, procedūras, kas paredzētas dublējumkopiju glabāšanai bezsaistē?	0		
	10					Vai jūs nosakāt pamata kiberdrošības pasākumus (obligātus vai ieteicamus) digitālo pakalpojumu sniedzējiem un visām TID direktīvas (Direktīva (ES) 2016/1148) II pielikumā minētajām nozarēm?	1				
	11	-		-		Vai jūs nodrošināt kiberincidentu atklāšanas rīkus vai metodikas?	1	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
12 – Apkarot kibernoziedzību	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumu, lai noteiktu, ar kādām tiesībaizsardzības prasībām (juridiskais pamats, resursi, prasmes utt.) var efektīvi apkarot kibernoziedzību?	1	Vai jūsu valsts tiesiskais regulējums pilnīgi atbilst attiecīgajam ES tiesiskajam regulējumam, tostarp Direktīvai 2013/40/ES par uzbrukumiem informācijas sistēmām, piemēram, attiecībā uz nelikumīgu piekļuvi informācijas sistēmām, nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datos, nelikumīgu pārtveršanu, rīkiem, ko izmanto nodarījumu izdarīšanai?	1	Vai jums ir kibernoziedzības lietu izskatīšanai veltītas vienības prokuratūrās?	1	Vai jūs vācat statistiku saskaņā ar Direktīvas 2013/40/ES (Direktīva par uzbrukumiem informācijas sistēmām) 14. panta 1. punkta noteikumiem?	1	Vai jums ir starpiestāžu apmācības vai apmācību darbsemināri tiesībaizsardzības iestādēm, tiesnešiem, prokuroriem un valsts/valdības *CSIRT* valsts un/vai daudzpusējā līmenī?	1
	2	Vai jūs esat veikuši pētījumu, lai noteiktu, ar kādām prokuroriem un tiesnešiem piemērojamām prasībām (juridiskais pamats, resursi, prasmes utt.) var efektīvi apkarot kibernoziedzību?	1	Vai jums ir kāda tiesību norma par tiešsaistes identitātes zādzību un persondatu zādzību?	1	Vai jums ir budžets, kas ir piešķirts tieši kibernoziedzības apkarošanas vienībām?	1	Vai jūs vācat atsevišķu statistiku par kibernoziedzību, piem., darbības statistiku, statistiku par kibernoziedzības tendencēm, statistiku par kibernoziedzībā iegūtiem līdzekļiem un radītajiem zaudējumiem?	1	Vai jūs piedalāties koordinētās starptautiska līmeņa darbībās, lai pārtrauktu noziedzīgas darbības, piem., iefiltrējaties noziedzīgos uzlaušanas forumos, organizētās kibernoziedzības grupās, tumšā tīmekļa tirgos un piedalāties robottīklu izjaukšanā?	1
	3	Vai jūsu valsts ir parakstījusi Eiropas Padomes Budapeštas konvenciju par kibernoziegumiem?	1	Vai jums ir kāda tiesību norma par tiešsaistes intelektuālā īpašuma tiesību un autortiesību pārkāpumiem?	1	Vai jūs esat izveidojuši centrālu struktūru/vienību, kas koordinē pasākumus kibernoziedzības apkarošanas jomā?	1	Vai jūs izvērtējat, cik noderīga kibernoziedzības apkarošanā ir tiesībaizsardzības iestāžu, tiesu iestāžu un valsts *CSIRT* darbiniekiem sniegtā apmācība?	1	Vai tad, kad *CSIRT*, tiesībaizsardzības iestādes un tiesu iestādes (prokurori un tiesneši) savā starpā sadarbojas, lai apkarotu kibernoziegumus, ir skaidri sadalīti pienākumi to starpā?	1
	4			Vai jums ir kāda tiesību norma par aizskaršanu vai iebiedēšanu tiešsaistē?	1	Vai jums ir izveidoti kibernoziedzības apkarošanā iesaistīto attiecīgo valsts iestāžu, tostarp tiesībaizsardzības iestāžu un valsts *CSIRT*, savstarpējās sadarbības mehānismi?	1	Vai jūs veicat regulārus izvērtējumus, lai pārliecinātos, ka tiesībaizsardzības iestāžu kibernoziedzības vienībām ir atvēlēts pietiekami daudz resursu (cilvēkresursu, budžeta un rīku)?	1	Vai jūsu normatīvais regulējums atvieglo sadarbību starp *CSIRT* / tiesībaizsardzības iestādēm un tiesu iestādēm (prokuroriem un tiesnešiem)?	1

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	R
12— Apkarot kibernoziedzību	5			Vai jums ir kāda tiesību norma par krāpšanu, kas saistīta ar datoriem, piemēram, par Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem noteikumu ievērošanu?	1	Vai jūs sadarbojaties un dalāties informācijā ar citām dalībvalstīm kibernoziedzības apkarošanas jomā?	1	Vai jūs veicat regulārus izvērtējumus, lai pārliecinātos, ka kriminālvajāšanas iestāžu kibernoziedzības vienībām ir atvēlēts pietiekami daudz resursu (cilvēkresursu, budžeta un rīku)?	1	Vai jūs piedalāties tādu standartizētu rīku un metodiku, veidlapu un procedūru veidošanā un uzturēšanā, kurus paredzēts kopīgot ar ES ieinteresētajām personām (tiesībaizsardzības iestādēm, *CSIRT*, *ENISA*, Eiropola *EC3* u. c.)?	1
	6	-		Vai jums ir kāda tiesību norma par bērnu aizsardzību internetā, piemēram, par Direktīvas 2011/93/ES un Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem noteikumu ievērošanu?	1	Vai jūs sadarbojaties un dalāties informācijā ar ES aģentūrām (piem., Eiropola *EC3*, *Eurojust*, *ENISA*) kibernoziedzības apkarošanas jomā?	1	Vai jums ir nodaļas, speciālas tiesas vai specializējušies tiesneši kibernoziedzības lietu izskatīšanai?	1	Vai jums ir ieviesti augsti attīstīti mehānismi, kas mazina personu vilinājumu iesaistīties kibernoziedzībā un attur personas no faktiskas iesaistīšanās tajā?	0
	7	-		Vai jūs esat noteikuši operatīvu valsts kontaktpunktu, ar kura starpniecību notiek informācijas apmaiņa un dalībvalstīm tiek sniegtas atbildes uz steidzamiem informācijas pieprasījumiem par nodarījumiem, kas minēti Direktīvā 2013/40/ES (Direktīva par uzbrukumiem informācijas sistēmām)?	1	Vai jums ir atbilstoši rīki kibernoziedzības apkarošanai, piem., kibernoziegumu taksonomija un klasifikācija, elektronisku pierādījumu vākšanas rīki, datorkriminālistikas rīki, uzticamas platformas informācijas kopīgošanai?	1	Vai jums ir kādi pasākumi, kas paredzēti atbalsta un palīdzības sniegšanai kibernoziegumos cietušajiem (parastajiem lietotājiem, MVU, lieliem uzņēmumiem)?	1	Vai jūsu valsts izmanto ES plānu un/vai tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokolu (*EU LE ERP*), lai efektīvi reaģētu uz plašapmēra kiberincidentiem?	0
	8			Vai jūsu tiesībaizsardzības iestādē ir īpaša kibernoziedzības apkarošanas vienība?	1	Vai jums ir standarta operāciju procedūras, kas nosaka, kā apieties ar e-pierādījumiem?	1	Vai jūs esat ieviesuši reaģēšanai uz kiberuzbrukumiem nepieciešamo starpiestāžu satvaru un mehānismus sadarbībai starp visām attiecīgajām ieinteresētajām personām (piem., tiesībaizsardzības iestādēm, valsts *CSIRT*, tiesu darbiniekiem), tostarp attiecīgā gadījumā arī ar privāto sektoru (piem., pamatpakalpojumu sniedzējiem, pakalpojumu sniedzējiem)?	1	-	
	9			Vai jūs saskaņā ar Budapeštas konvencijas 35. pantu esat izveidojuši kontaktpunktu, kas pieejams 24 stundas diennaktī, 7 dienas nedēļā?	1	Vai jūsu valsts izmanto apmācības iespējas, ko piedāvā un/vai atbalsta ES aģentūras (piem., Eiropols, *Eurojust*, *OLAF*, *CEPOL*, *ENISA*)?	0	Vai jūsu normatīvais regulējums atvieglo sadarbību starp *CSIRT* un tiesībaizsardzības iestādēm?	1	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
12 – Apkarot kibernoziedzību	10	-		Vai jūs ES tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokola (*EU LE ERP*) vajadzībām esat iecēluši operatīvu valsts kontaktpunktu, kas darbojas 24 stundas diennaktī, 7 dienas nedēļā un ko izmanto reaģēšanā uz lieliem kiberuzbrukumiem?	1	Vai jūsu valsts apsver iespēju pieņemt Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem otro papildu protokolu?	0	Vai jums ir ieviesti mehānismi (piem., rīki, procedūras), ar ko atvieglot informācijas apmaiņu un sadarbību starp *CSIRT* / tiesībaizsardzības iestādēm un, iespējams, tiesu iestādēm (prokuroriem un tiesnešiem) kibernoziedzības apkarošanas jomā?	1	-	
	11			Vai jūs regulāri sniedzat speciālu apmācību ieinteresētajām personām, kas ir iesaistītas kibernoziedzības apkarošanā (tiesībaizsardzības iestādēm, tiesu iestādēm, *CSIRT*), piem., nodarbības, kas attiecas uz apsūdzības celšanu par noziegumiem, kurus padara iespējamus kibertelpa, vai uz krimināvajāšanu par šādiem noziegumiem, apmācības par elektronisku pierādījumu vākšanu un to, kā nodrošināt integritāti visā digitālajā pārraudzības ķēdē un datorkriminālistikā.	1						
	12			Vai jūsu valsts ir ratificējusi Eiropas Padomes Budapeštas konvenciju par kibernoziegumiem vai pievienojusies tai?	1			-	-	-	
	13	-		Vai jūsu valsts ir parakstījusi un ratificējusi Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem papildu protokolu (rasisma un ksenofobijas noziedzīgie nodarījumi, kas tiek izdarīti datorsistēmās)?	0	-	-	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
13 – Izveidot mehānismus ziņošanai par incidentiem	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jums ir neformāli mehānismi informācijas par kiberdrošības incidentiem apmaiņai starp privātām organizācijām un valsts iestādēm?	1.	Vai jums ir sistēma ziņošanai par incidentiem visās TID direktīvas II pielikumā minētajās nozarēs?	1	Vai jums ir obligātas ziņošanas par incidentiem sistēma, kas darbojas praksē?	1	Vai jums ir saskaņota procedūra nozaru sistēmām, kas paredzētas ziņošanai par incidentiem?	1	Vai jūs sagatavojat ikgadējo ziņojumu par incidentiem?	1
	2	-		Vai jūs esat ieviesuši paziņošanas prasības telesakaru pakalpojumu sniedzējiem saskaņā ar Direktīvas (ES) 2018/1972 40. pantu? Direktīvā dalībvalstīm ir noteikta prasība nodrošināt, ka publisko elektronisko sakaru tīklu vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji bez liekas kavēšanās paziņo kompetentajai iestādei par drošības incidentiem, kas ir būtiski ietekmējuši tīklu darbību vai pakalpojumu sniegšanu.	1	Vai ir koordinācijas/sadarbības mehānisms saistībā ar ziņošanas par incidentiem pienākumiem, kas noteikti VDAR, TID direktīvā, 40. pantā (agrākajā 13.a pantā) un *eIDAS*?	1	Vai jums ir sistēma ziņošanai par incidentiem nozarēs, kas nav minētas TID direktīvā?	1	Vai ir ieviesti ziņojumi par kiberdrošības ainu vai citu veidu analīze, ko sagatavo struktūra, kura saņem ziņojumus par incidentiem?	1
	3	-		Vai jūs esat ieviesuši paziņošanas prasības uzticamības pakalpojumu sniedzējiem saskaņā ar *eIDAS* regulas (Regula (ES) Nr. 910/2014) 19. pantu? 19. pantā cita starpā ir noteikts, ka uzticamības pakalpojumu sniedzējiem ir jāpaziņo uzraudzības iestādei par būtiskiem incidentiem / drošības pārkāpumiem.	1	Vai jums ir atbilstoši rīki, ar ko nodrošināt pa dažādiem ziņošanas kanāliem paziņotās informācijas konfidencialitāti un integritāti?	1	Vai jūs mērāt ziņošanas par incidentiem procedūru efektivitāti, piem., izmantojat rādītājus par incidentiem, par kuriem ir ziņots pa atbilstošiem kanāliem, ziņošanas par incidentiem savlaicīguma rādītājus?	1	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
13 – Izveidot mehānismus ziņošanai par incidentiem	4	-		Vai jūs esat ieviesuši paziņošanas prasības digitālo pakalpojumu sniedzējiem saskaņā ar TID direktīvas 16. pantu? 16. pantā ir noteikts, ka digitālo pakalpojumu sniedzējiem bez nepamatotas kavēšanās jāpaziņo kompetentajai iestādei vai valsts *CSIRT* par jebkuru incidentu, kuram ir būtiska ietekme uz tā pakalpojuma sniegšanu, kas minēts III pielikumā un ko tie piedāvā Savienībā.	1	Vai jums ir platforma/rīks, kas atvieglo ziņošanas procesu?	0	Vai jums ir kopēja valsts līmeņa taksonomija incidentu klasifikācijai un pirmcēloņu kategorijām?	0	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
14 – Pastiprināt privātuma un datu aizsardzību	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jūs esat veikuši pētījumus vai analīzes, lai noteiktu, kuras jomas ir jāuzlabo, lai labāk aizsargātu iedzīvotāju tiesības uz privātumu?	1	Vai valsts datu aizsardzības iestāde ir iesaistīta ar kiberdrošību saistītu jautājumu risināšanā (piem., jaunu kiberdrošības normatīvo aktu izstrādē, minimālo drošības pasākumu noteikšanā)?	1	Vai jūs veicināt drošības pasākumu un integrētās datu aizsardzības paraugpraksi publiskajā un/vai privātajā sektorā?	1	Vai jūs veicat regulārus izvērtējumus, lai pārliecinātos, ka datu aizsardzības iestādei ir atvēlēts pietiekami daudz resursu (cilvēkresursu, budžeta un rīku)?	1	Vai jums ir ieviesti mehānismi tehnoloģiju attīstības jaunāko pavērsienu uzraudzībai, lai varētu attiecīgi pielāgot atbilstošās pamatnostādnes un tiesību normas / juridiskos pienākumus?	1
	2	Vai jūs valsts līmenī esat izstrādājuši juridisko pamatu Vispārīgās datu aizsardzības regulas (Regula (ES) 2016/679) izpildei, piem., saglabājuši regulas noteikumus vai ieviesuši sīkāk izstrādātus noteikumus vai ierobežojumus, nekā paredzēts regulā?	0	-		Vai jūs īstenojat izpratnes vairošanas un apmācību programmas par šo tematu?	1	Vai jūs mudināt organizācijas un uzņēmumus saņemt ISO/IEC 27701:2019 sertifikātu attiecībā uz privātās informācijas pārvaldības sistēmu (*PIMS*)?	1	Vai jūs aktīvi piedalāties privātuma aizsardzības tehnoloģiju (*PET*) pētniecības un izstrādes iniciatīvās vai veicināt tās?	0
	3	-		-		Vai jūs saskaņojat ziņošanas par incidentiem procedūras ar datu aizsardzības iestādi?	1	-		-	
	4	-		-		Vai jūs veicināt un atbalstāt informācijas drošības un privātuma tehnisko standartu izstrādi? Vai tie ir pielāgoti tieši maziem un vidējiem uzņēmumiem (MVU)?	0	-		-	
	5	-		-		Vai jūs sniedzat praktiskas un mērogojamas pamatnostādnes, lai palīdzētu dažādu veidu datu pārziņiem izpildīt tiesību aktos noteiktās prasības un pienākumus, kas attiecas uz privātuma un datu aizsardzību?	0	-		-	

4.1.4 4. grupa: sadarbība

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
15 – Izveidot publiskā un privātā sektora partnerību (PPP)	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai valda uzskats, ka PPP ar dažādiem līdzekļiem palīdz paaugstināt kiberdrošības līmeni valstī, piem., īsteno kopīgas intereses veicināt kiberdrošības nozares izaugsmi, sadarbojas attiecīga kiberdrošības normatīvā regulējuma veidošanā, veicina pētniecību un izstrādi?	1	Vai jums ir valsts rīcības plāns PPP izveidei?	1	Vai jūs esat izveidojuši publiskā un privātā sektora valsts partnerības?	1	Vai jūs esat izveidojuši pārnozaru PPP?	1	Vai jūs spējat pielāgot vai izveidot PPP, ņemot vērā jaunākās izmaiņas tehnoloģiju jomā un normatīvajā regulējumā?	1
	2	-		Vai jūs izveidojat juridisku vai līgumisku pamatu (īpaši tiesību akti, informācijas neizpaušanas līgumi, intelektuālais īpašums), lai noteiktu PPP darbības jomu?	1	Vai jūs esat izveidojuši nozares PPP?	1	Vai jūs izveidotajās PPP pievēršaties arī publiskā sektora dalībnieku savstarpējai sadarbībai un privātā sektora dalībnieku savstarpējai sadarbībai?	1		
	3	-		-		Vai jūs nodrošināt finansējumu PPP izveidei?	1	Vai jūs veicināt PPP veidošanu starp maziem un vidējiem uzņēmumiem (MVU)?	1	-	
	4	-		-		Vai publiskā sektora iestādes kopumā vada PPP, t. i., viens vienots publiskā sektora kontaktpunkts pārvalda un koordinē PPP, publiskā sektora struktūras iepriekš vienojas par to, ko tās vēlas sasniegt, valsts pārvaldes iestādes sniedz skaidrus norādījumus privātajam sektoram par savām vajadzībām un ierobežojumiem, utt.?	1	Vai jūs mērāt PPP darbības rezultātus?	1	-	
	5	-		-		Vai jūs piedalāties Eiropas Kiberdrošības organizācijas (*ECSO*) līgumiskajā publiskā un privātā sektora partnerībā?	0	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
15 – Izveidot publiskā un privātā sektora partnerību (PPP)	6	-		-		Vai jums ir viena vai vairākas PPP, kuru darbs attiecas uz *CSIRT* darbībām?	0	-		-	
	7					Vai jums ir viena vai vairākas PPP, kuru darbs attiecas uz informācijas kritiskās infrastruktūras aizsardzības jautājumiem?	0				
	8	-		-		Vai jums ir viena vai vairākas PPP, kuru darbs attiecas uz kiberjautājumu izpratnes vairošanu un prasmju pilnveidi?	0	-		-	

VKS mērķis	Nr.	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
16 – Institucionalizēt sadarbību starp publiskā sektora aģentūrām	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jums ir neformāli kanāli, ko publiskā sektora aģentūras izmanto savstarpējai sadarbībai?	1	Vai jums ir uz kiberdrošību vērsta valsts sadarbības shēma, piem., konsultatīvās padomes, vadības grupas, forumi, padomes, kiberdrošības centri vai ekspertu sanāksmju grupas?	1	Vai publiskā sektora iestādes piedalās sadarbības shēmā?	1	Vai jūs nodrošināt, ka kiberdrošībai veltīti sadarbības kanāli pastāv vismaz starp šādām publiskā sektora struktūrām: izlūkošanas dienestiem, iekšzemes tiesībaizsardzības iestādēm, kriminālvajāšanas iestādēm, valdības pārstāvjiem, valsts *CSIRT* un militārpersonām?	1	Vai publiskā sektora aģentūrām tiek sniegta vienāda minimālā informācija par jaunākajām izmaņām apdraudējumu ainā un kiberdrošības situācijas apzināšanos?	1
	2	-		-		Vai jūs esat izveidojuši informācijas apmaiņai paredzētas sadarbības platformas?	1	Vai jūs mērāt dažādu sadarbības shēmu panākumus un ierobežojumus efektīvas sadarbības veicināšanā?	1	-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
16 – Institucionalizēt sadarbību starp publiskā sektora aģentūrām	3	-		-		Vai jūs esat noteikuši sadarbības platformu darbības jomu (piem., uzdevumus un pienākumus, problēmjomu skaitu)?	1	-		-	
	4	-		-		Vai jūs organizējat ikgadējas sanāksmes?	1	-		-	
	5	-		-		Vai jums ir mehānismi sadarbībai starp kompetentajām iestādēm, kas atrodas dažādos ģeogrāfiskajos reģionos, piem., reģionālo drošības korespondentu tīkls, kiberdrošības speciālists reģionālajās ekonomikas palātās?	1	-		-	

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
17 – Iesaistīties starptautiskajā sadarbībā (ne tikai ar ES dalībvalstīm)	a	Vai šis mērķis jau ir ietverts jūsu VKS, vai arī jūs plānojat to ietvert nākamajā tās redakcijā?	1	Vai pastāv neformāla prakse vai pasākumi, kas palīdz sasniegt šo mērķi nekoordinētā veidā?	1	Vai jums ir oficiāli noteikts un dokumentēts rīcības plāns?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai pārbaudītu tā rezultātus?	1	Vai jums ir ieviesti mehānismi, ar ko nodrošināt, ka rīcības plāns tiek dinamiski pielāgots izmaiņām apkārtējā vidē?	1
	b			Vai jūs savam rīcības plānam esat noteikuši gaidāmos rezultātus, pamatprincipus vai galvenos pasākumus?	1	Vai jūsu rīcības plānam ir skaidrs resursu piešķīrums un pārvaldība?	1	Vai jūs pārskatāt savu rīcības plānu attiecībā uz šo mērķi, lai nodrošinātu, ka tiek pareizi noteiktas tā prioritātes un tas tiek optimizēts?	1		
	c			Ja attiecas — vai jūsu rīcības plāns ir ieviests un jau faktiski tiek īstenots ierobežotā apjomā?	0						
	1	Vai jums ir stratēģija, kā iesaistīties starptautiskā līmenī?	1	Vai jums ir noslēgti sadarbības nolīgumi ar citām valstīm (divpusēji, daudzpusēji) vai partneriem citās valstīs, piem., par informācijas kopīgošanu, spēju veidošanu, palīdzību?	1	Vai jūs apmainās ar stratēģisku informāciju, piem., par augsta līmeņa politiku, riska uztveri?	1	Vai jūsu valsts publiskā sektora kiberdrošības aģentūras ir iesaistījušās starptautiskās sadarbības shēmās?	1	Vai jūs vadāt diskusijas par vienu vai daudziem tematiem daudzpusēju nolīgumu ietvaros?	1
	2	Vai jums ir neformāli kanāli sadarbībai ar citām valstīm?	1	Vai jums ir vienots kontaktpunkts, kas var veikt koordinatora funkciju, lai nodrošinātu pārrobežu sadarbību ar dalībvalstu iestādēm (sadarbības grupa, *CSIRT* tīkls utt.)?	1	Vai jūs apmainās ar taktisku informāciju (piem., apdraudētāju biļetens, informācijas apmaiņas un analīzes centri, taktika, paņēmieni un procedūras (*TTP*))?	1	Vai jūs regulāri novērtējat starptautiskās sadarbības iniciatīvu iznākumu?	1	Vai jūs vadāt diskusijas par vienu vai daudziem tematiem starptautisku līgumu vai konvenciju ietvaros?	1

VKS mērķis	#	1. līmenis	O	2. līmenis	O	3. līmenis	O	4. līmenis	O	5. līmenis	O
17 – Iesaistīties starptautiskajā sadarbībā (ne tikai ar ES dalībvalstīm)	3	Vai publiskā sektora vadošie dalībnieki ir pauduši nodomu iesaistīties starptautiskajā sadarbībā kiberdrošības jomā?	1	Vai jūsu valstī starptautiskajā sadarbībā iesaistās cilvēki, kas ir īpaši izraudzīti šim mērķim?	1	Vai jūs apmainās ar operatīvu informāciju, piem., operatīvu koordinācijas informāciju, informāciju par notiekošiem incidentiem, aizskāruma rādītājiem?	1	-		Vai jūs vadāt diskusijas vai sarunas par vienu vai daudziem tematiem starptautiskās ekspertu grupās, piem., Globālajā kibertelpas stabilitātes komisijā (*GCSC*), *ENISA*, TID sadarbības grupā, ANO Informācijas drošības valdības ekspertu grupā?	1
	4	-		-		Vai jūs iesaistāties starptautiskās kiberdrošības mācībās?	1	-		-	
	5	-		-		Vai jūs iesaistāties starptautiskās spēju veidošanas iniciatīvās, piem., apmācībās, spēju pilnveidošanā, standarta procedūru izstrādē?	0	-		-	
	6	-		-		Vai jūs esat noslēguši savstarpējās palīdzības nolīgumus ar citām valstīm, piem., par tiesībaizsardzības iestāžu darbībām, tiesvedību, reaģēšanas uz incidentiem spēju kopīgošanu, dalīšanos ar kiberdrošības līdzekļiem?	0	-		-	
	7	-		-		Vai jūs esat parakstījuši vai ratificējuši starptautiskus līgumus vai konvencijas kiberdrošības jomā, piem., Starptautisko rīcības kodeksu informācijas drošības jomā, Konvenciju par kibernoziegumiem?	0	-		-	

4.2 NORĀDES PAR SISTĒMAS IZMANTOŠANU

Šīs iedaļas mērķis ir sniegt dalībvalstīm norādes un ieteikumus par to, kā ieviest sistēmu un aizpildīt anketu. Tālāk uzskaitītie ieteikumi lielākoties izriet no komentāriem, kas tika saņemti intervijās ar dalībvalstu pārstāvjiem.

- **Paredziet koordinācijas pasākumus datu vākšanai un konsolidēšanai.** Vairums dalībvalstu atzīst, ka šāda pašnovērtējuma veikšanai varētu būt vajadzīgs aptuveni 15 cilvēkdienu. Lai veiktu pašnovērtējumu, būs jāiesaista daudz dažādu ieinteresēto personu. Tāpēc ir ieteicams atvēlēt laiku sagatavošanās posmam, kurā nosaka visas attiecīgās ieinteresētās personas valdības struktūrās, publiskā sektora aģentūrās un privātajā sektorā.
- **Ieceliet centralizētu struktūru, kas būs atbildīga par pašnovērtējuma veikšanu valsts mērogā.** Lai savāktu materiālus visiem VSNS rādītājiem, varētu būt jāiesaista daudz ieinteresēto personu, tāpēc ir ieteicams uzdot centrālai struktūrai vai aģentūrai veikt šo pašnovērtējumu, sazinoties un saskaņojot rīcību ar visām attiecīgajām ieinteresētajām personām.
- **Izmantojiet novērtēšanas procesu, lai sniegtu informāciju un apmainītos ar informāciju par kiberdrošības jautājumiem.** Pieredze, ar ko dalībvalstis dalījās, liecina, ka diskusijas (kas norisinās vai nu individuālās intervijās vai kolektīvos darbsemināros) ir laba iespēja veicināt dialogu par kiberdrošības jautājumiem, rast kopsaucēju un apzināt jomas, kurās nepieciešami uzlabojumi. Daloties ar rezultātiem, var ne tikai izcelt svarīgākos sasniegumus, bet arī vairot izpratni par kiberdrošības jautājumiem.
- **Izmantojiet VKS par mērauklu novērtējamo mērķu atlasē.** VSNS ietilpstošie 17 mērķi tikai formulēti, pamatojoties uz mērķiem, ko dalībvalstis bieži vien bija ietvērušas savās VKS. VKS ietvertie mērķi būtu jāizmanto par atsauci novērtējuma tvēruma noteikšanā. Tomēr VKS nevajadzētu ierobežot novērtējumu. Tā kā VKS, protams, pievēršas prioritātēm, dažas jomas ar nodomu nav iekļautas VKS. Tomēr tas nenozīmē, ka valstij attiecīgo spēju nav. Piemēram, ja konkrēts mērķis VKS nav iekļauts, bet valstij ir ar šo mērķi saistītas kiberdrošības spējas, šo mērķi var novērtēt.
- **Kad VKS tvērums mainās, pārliecinieties, ka vērtējuma interpretācija mainās līdz ar VKS.** VKS dzīves cikls ilgst vairākus gadus. Dažās dalībvalstīs VKS īstenošanai parasti ir paredzēts 3–5 gadu ceļvedis un divas secīgas VKS pēc sava tvēruma viena no otras vairāk vai mazāk atšķiras. Ņemot to vērā, ir jābūt īpaši piesardzīgiem, iepazīstinot ar divu atšķirīgu VKS pašnovērtējuma rezultātiem, jo tvēruma izmaiņas var ietekmēt galīgo gatavības vērtējumu. Ir ieteicams pa gadiem salīdzināt tos vērtējumus, kas attiecas uz visu stratēģisko mērķu kopumu (t. i., kopējo vispārējo vērtējumu).

Atgādinājums par vērtējuma piešķiršanas mehānismu — aptvēruma pakāpes piemērs
Vērtējuma piešķiršanas mehānismam ir divi vērtējumu līmeņi:
(i) **kopējā vispārējā aptvēruma pakāpe**, kas ir balstīta uz visiem pašnovērtēšanas sistēmā ietvertajiem stratēģiskajiem mērķiem, un
(ii) **kopējā konkrētā aptvēruma pakāpe**, kas ir balstīta uz dalībvalsts izvēlētajiem stratēģiskajiem mērķiem (tie parasti ir konkrētās valsts VKS ietvertie mērķi).

Mehānisma uzbūves dēļ (sk. 3.1. iedaļu par vērtējuma piešķiršanas mehānismu) kopējā konkrētā aptvēruma pakāpe ir vienāda ar kopējo vispārējo aptvēruma pakāpi vai augstāka par to, jo kopējā vispārējā aptvēruma pakāpe var ietvert mērķus, kurus dalībvalsts nav izvēlējusies, un tāpēc šīs pakāpes vērtējums var pazemināties. Ja dalībvalsts pievieno jaunu mērķi, kopējā aptvēruma pakāpe paaugstinās (t. i., tiek aptverts vairāk gatavības rādītāju), savukārt kopējā konkrētā gatavība var samazināties (ja no jauna pievienotais mērķis ir sākumposmā, kā dēļ tam ir zemāks gatavības līmenis).

- **Aizpildot pašnovērtējuma anketu, paturiet prātā, ka galvenais mērķis ir palīdzēt dalībvalstīm veidot kiberdrošības spējas.** Tāpēc, lai arī dažās situācijās var būt grūti uz jautājumu dot skaidru atbildi, veicot pašnovērtējumu, ieteicams izvēlēties to atbildi, par ko ir lielāka vienprātība. Ja, piemēram, atbilde uz jautājumu vienos aspektos ir "JĀ", bet citos — "NĒ", dalībvalstīm vajadzētu atcerēties, ka atbilde "NĒ" nozīmē, ka kaut kas ir jādara — jāsagatavo koriģējošu pasākumu plāns vai rīcības plāns kādā jomā, kur nepieciešami uzlabojumi, — un šī vajadzība jāņem vērā turpmākajā rīcībā nākotnē.

5. NĀKAMIE SOĻI

5.1 TURPMĀKI UZLABOJUMI

Intervijās ar dalībvalstu pārstāvjiem un dokumentu izpētes posmā tika noteikti arī šādi ieteikumi pašreizējās valsts spēju novērtēšanas sistēmas uzlabošanai, ko varētu veikt nākotnē.

- **Pilnveidot vērtējuma piešķiršanas sistēmu, lai tā dotu precīzāku rezultātu.** Piemēram, binārās "JĀ/NĒ" atbildes vietā varētu ieviest procentuālo izpildes rādītāju, lai labāk ņemtu vērā to, cik sarežģīti ir konsolidēt spējas valsts līmenī. Šī vienkāršā pieeja ar "JĀ/NĒ" atbildēm tika izvēlēta kā sākotnējais variants.
- **Ieviest kvantitatīvus rādītājus dalībvalstu VKS efektivitātes novērtēšanai.** Valsts spēju novērtēšanas sistēma pievēršas dalībvalstu kiberdrošības spēju gatavības līmeņa izvērtēšanai. To varētu papildināt ar rādītājiem, kuri parādītu, cik efektīvi ir pasākumi un rīcības plāni, ko dalībvalstis īstenojušas šo spēju veidošanas nolūkā. Nešķita reāli izveidot šādus efektivitātes rādītājus pašreizējā posmā, jo ir saņemts maz atsauksmju no nozares, ir grūti atrast vērtīgus rādītājus, kas sasaistītu iznākumu ar VKS īstenošanu, un ir grūti izveidot reālistiskus rādītājus, kuriem vajadzīgo informāciju pēc tam var faktiski apkopot. Taču šis jautājums tiks ņemts vērā turpmākajā darbā.
- **Pāriet no pašnovērtēšanas un novērtēšanu.** Vienas no iespējamajām sistēmas izmaiņām nākotnē varētu būt pāriešana uz novērtēšanas pieeju, lai novērtētu dalībvalstu kiberdrošības spēju gatavību konsekventāk. Uzdodot novērtējumu veikt trešai personai, patiešām varētu samazināt iespējamo neobjektivitāti.

A PIELIKUMS. PĀRSKATS PAR DOKUMENTU IZPĒTES REZULTĀTIEM

A pielikumā ir rezumēts ar VKS saistītais darbs, ko *ENISA* veikusi iepriekš, un sniegts pārskats par attiecīgiem publiski pieejamiem kiberdrošības spēju gatavības modeļiem. Modeļu atlasē un pārskatīšanā tika ņemti vērā šādi apsvērumi:

- ne visi modeļi ir balstīti uz rūpīgi izstrādātu izpētes metodiku;
- modeļu struktūra un rezultāti ne vienmēr ir pienācīgi izskaidroti, un ne vienmēr ir skaidri norādītas saiknes starp dažādajiem katra modeļa elementiem;
- daži modeļi nesniedz informāciju par izstrādes procesu, struktūru un novērtēšanas metodiku;
- citi mūsu atrasti modeļi un rīki nesniedz nekādu informāciju par struktūru un saturu, un tāpēc tie netika iekļauti sarakstā;
- pārskatāmie modeļi tika atlasīti, ņemot vērā ģeogrāfisko tvērumu. Galvenā uzmanība tiks pievērsta kiberdrošības spēju gatavības modeļiem, kas veidoti tā, lai varētu novērtēt Eiropas valstu rezultātus. Taču ir svarīgi paplašināt ģeogrāfisko tvērumu, lai analizētu labu praksi gatavības modeļu veidošanā visā pasaulē.

Publiski pieejami, attiecīgi kiberdrošības spēju gatavības modeļi tika sistemātiski pārskatīti, izmantojot pielāgotu analīzes satvaru, kas balstīts uz Bekera [*Becker*] formulēto metodiku gatavības modeļu izstrādei[22]. Tika analizēti šādi katra pastāvošā gatavības modeļa elementi:

- **gatavības modeļa nosaukums:** gatavības modeļa nosaukums un galvenās atsauces;
- **avotinstitūcija:** publiskā vai privātā sektora institūcija, kas ir atbildīga par modeļa izstrādi;
- **galvenais mērķis un mērķauditorija:** modeļa kopējais tvērums un paredzētā(-ās) mērķauditorija(-as);
- **līmeņu skaits un definīcija:** modeļa gatavības līmeņu skaits, kā arī to vispārīgais apraksts;
- **atribūtu skaits un nosaukums:** gatavības modelī izmantoto atribūtu skaits un nosaukums. Atribūtu analīzei ir trīs mērķi:
  - sadalīt gatavības modeli viegli saprotamās sīkākās daļās;
  - apvienot vairākus atribūtus ar vienu un to pašu mērķi atribūtu grupās;
  - aplūkot gatavības līmeņa priekšmetu dažādos aspektos;
- **novērtēšanas metode:** gatavības modeļa novērtēšanas metode;
- **rezultātu atspoguļojums:** noteikt gatavības modeļa rezultātu vizualizācijas metodi. Šīs darbības iemesls ir tāds, ka gatavības modeļi parasti nav sekmīgi, ja tie ir pārāk sarežģīti, tāpēc atspoguļojuma veidam ir jāatbilst praktiskām vajadzībām.

[22] Becker, J., Knackstedt, R., un Pöppelbuß, J., "Developing Maturity Models for IT Management: A Procedure Model and its Application", *Business & Information Systems Engineering*, 1. sēj., Nr. 3, 213.–222. lpp., 2009. gada jūnijs.
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

Iepriekšējs darbs VKS jomā

ENISA agrīnie centieni ietvēra divus dokumentus par VKS tēmu, kuri tika publicēti 2012. gadā. Pirmkārt, praktiskajos norādījumos "Practical guide on the development and execution phase of NCSS"[23] tika ierosināts vairāku konkrētu darbību kopums efektīvai VKS īstenošanai un tika aprakstīts VKS dzīves cikls, kas sastāv no četriem posmiem: stratēģijas izstrāde, stratēģijas izpilde, stratēģijas izvērtēšana un stratēģijas uzturēšana. Otrkārt, dokumentā "Setting the course for national efforts to strengthen security in cyberspace"[24] tika izklāstīta kiberdrošības stratēģiju situācija ES un citviet 2012. gadā un dalībvalstīm tika ieteikts noteikt kopīgas tēmas un atšķirības starp to VKS.

2014. gadā tika publicēta pirmā *ENISA* dalībvalsts VKS izvērtēšanas sistēma[25]. Minētajā sistēmā ir iekļauti ieteikumi un laba prakse, kā arī spēju veidošanas rīku kopums VKS izvērtēšanai (piem., noteiktie mērķi, resursi, rezultāti, galvenie darbības rādītāji). Šie rīki ir pielāgoti dažādajām vajadzībām, kas ir valstīm ar atšķirīgu gatavības līmeni stratēģiskajā plānošanā. Tai pašā gadā *ENISA* publicēja VKS interaktīvo tiešsaistes karti[26], kurā lietotāji var ātri aplūkot visu dalībvalstu un EBTA valstu VKS, tostarp to stratēģiskos mērķus un labus īstenošanas piemērus. Tā sākotnēji (2014. gadā) tika izstrādāta kā VKS repozitorijs, bet pēc tam, 2018. gadā, tika papildināta ar īstenošanas piemēriem, un kopš 2019. gada karte ir *informācijas centrs*, kurā tiek centralizēti apkopti dalībvalstu sniegtie dati par to centieniem uzlabot valsts kiberdrošību.

2016. gadā publicētajā ceļvedī "NCSS Good Practice Guide"[27] ir noteikti 15 stratēģiskie mērķi. Minētajā ceļvedī ir arī analizēts katras dalībvalsts VKS īstenošanas statuss un noteiktas dažādas nepilnības un grūtības to īstenošanā.

Pēc tam *ENISA* 2018. gadā publicēja Valstu kiberdrošības stratēģiju izvērtēšanas rīku[28] — interaktīvu pašnovērtēšanas rīku, kuru dalībvalstis var izmantot, lai izvērtētu savas stratēģiskās prioritātes un mērķus, kas saistīti ar to VKS. Ar šo rīku dalībvalstis, atbildot uz vienkāršiem jautājumiem, var saņemt konkrētus ieteikumus katra mērķa īstenošanai. Visbeidzot, 2019. gadā publicētajā dokumentā "Good practices in innovation on Cybersecurity under the NCSS"[29] ir aplūkots jautājums par inovāciju kiberdrošības jomā VKS kontekstā. Dokumentā, pamatojoties uz jomas ekspertu viedokli, ir izklāstītas problēmas un laba prakse dažādos inovācijas aspektos, lai palīdzētu izstrādāt turpmākus inovatīvus stratēģiskos mērķus.

A.1 Kiberdrošības spēju gatavības modelis valstīm (*CMM*)

Kiberdrošības spēju gatavības modeli valstīm (*CMM*) ir izstrādājis Globālais kiberdrošības spēju centrs (tālāk "Spēju centrs"), kas pieder pie Oksfordas Universitātes Oksfordas Mārtina skolas. Spēju centra mērķis ir palielināt kiberdrošības spēju veidošanas apmēru un efektivitāti gan Apvienotajā Karalistē, gan starptautiskā mērogā, izvēršot Kiberdrošības spēju gatavības modeli

[23] *NCSS: Practical Guide on Development and Execution* (*ENISA*, 2012), https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
[24] *NCSS: Setting the course for national efforts to strengthen security in cyberspace* (*ENISA*, 2012), https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.
[25] *An evaluation framework for NCSS* (*ENISA*, 2014), https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.
[26] Valstu kiberdrošības stratēģijas — interaktīva karte (*ENISA*, 2014, atjaunināta 2019. gadā), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[27] Ar šo dokumentu tiek atjaunināti 2012. gada norādījumi "NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies" (*ENISA*, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[28] Valstu kiberdrošības stratēģiju izvērtēšanas rīks (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.

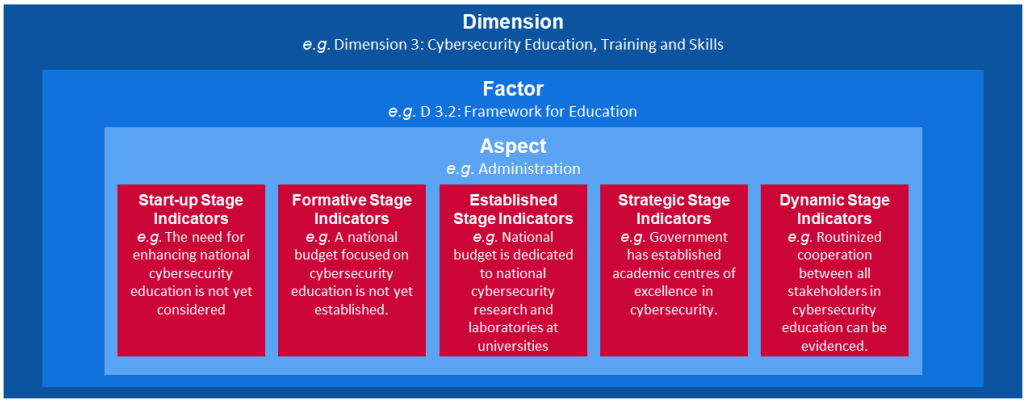
(*CMM*). *CMM* ir paredzēts tieši tām valstīm, kas vēlas paaugstināt savas valsts kiberdrošības spējas. *CMM* pirmoreiz tika ieviests 2014. gadā; pēc tam 2016. gadā, kad tas bija izmantots 11 valstu kiberdrošības spēju novērtēšanai, *CMM* tika pārskatīts.

Atribūti/virzieni

CMM tiek pieņemts, ka kiberdrošības spējas sastāv no **pieciem virzieniem**, kas atspoguļo kiberdrošības spēju grupas. Katra grupa ir atšķirīga izpētes "prizma", caur kuru var pētīt un izprast kiberdrošības spējas. Visos piecos virzienos **faktori** detalizēti apraksta, kā izpaužas kiberdrošības spēju esība. Šīs detaļas ir elementi, kas palīdz paaugstināt kiberdrošības spēju gatavību katrā virzienā. Katra faktora dažādās sastāvdaļas atspoguļo vairāki **aspekti**. Aspekti rodas, sakārtojot rādītājus mazākās grupās, ko ir vieglāk aptvert. Pēc tam katru aspektu izvērtē ar **rādītājiem**, kuri apraksta soļus, darbības vai veidojošos elementus, kas liecina par konkrētu gatavības pakāpi (tās aprakstītas nākamajā iedaļā) atsevišķā aspektā, faktorā un virzienā.

Iepriekš minētos jēdzienus var sakārtot slāņos, kā parādīts nākamajā attēlā.

4. attēls. *CMM* rādītāju piemērs



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills
Factor
e.g. D 3.2: Framework for Education
Aspect
e.g. Administration
Start-up Stage Indicators
e.g. The for enhancing national cybersecurity education is not yet considered
Formative Stage Indictors
e.g. A national budget focused on cybersecurity education is not yet established
Established Stage Indicators
e.g. National budget is dedicated to national cybersecurity research and laboratories at universities
Strategic Stage Indicators
e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.
Dynamic Stage Indicators
e.g. Routinized cooperation between all stakeholder

Virziens
Piem., 3. virziens "Kiberdrošības izglītība, apmācība un prasmes"
Faktors
Piem., D 3.2 "Izglītības satvars"
Aspekts
Piem., administrēšana
Sākumposma rādītāji
Piem., vajadzība uzlabot valsts kiberdrošības izglītību vēl nav apsvērta
Veidošanās posma rādītāji
Piem., uz kiberdrošības izglītību vērsts valsts budžets vēl nav noteikts
Nostiprināšanās posma rādītāji
Piem., ir paredzēts valsts budžets valsts kiberdrošības pētniecībai un laboratorijām universitātēs
Stratēģiskā posma rādītāji
Piem., valdība ir izveidojusi akadēmiskos izcilības centrus kiberdrošības jomā
Dinamiskā posma rādītāji
Piem., var novērot regulāru sadarbību starp visām ieinteresētajām personām kiberdrošības izglītības jomā

Pieci minētie virzieni ir šādi:

i kiberdrošības politikas un stratēģijas izstrāde (seši faktori);
ii atbildīgas kiberdrošības kultūras veicināšana sabiedrībā (pieci faktori);
iii kiberdrošības zināšanu pilnveidošana (trīs faktori);
iv iedarbīga tiesiskā un normatīvā regulējuma izveide (trīs faktori);
v risku kontrolēšana, izmantojot standartus, organizācijas un tehnoloģijas (septiņi faktori).

Gatavības līmeņi

CMM izmanto **piecus gatavības līmeņus**, lai noteiktu, cik lielu progresu valsts ir panākusi attiecībā uz konkrētu kiberdrošības spēju faktoru/aspektu. Šie līmeņi atspoguļo pastāvošās kiberdrošības spējas konkrētā laikā:

- **sākumposms**. Šajā posmā vai nu nav nekādu kiberdrošības spēju, vai arī tās ir pašā iedīglī. Var būt aizsākušās sākotnējas diskusijas par kiberdrošības spēju veidošanu, bet nekādas konkrētas darbības vēl nav veiktas. Šajā posmā nav novērojami nekādi pierādījumi;
- **veidošanās posms**. Dažas aspektu daļas ir sākušas augt un veidoties, taču tām, iespējams, pievēršas tikai pēc vajadzības, tās var būt dezorganizētas, slikti noteiktas vai vienkārši "jaunas". Taču ir skaidri redzami pierādījumi par šādām darbībām;
- **nostiprināšanās posms**. Aspekta elementi ir ieviesti un darbojas. Tomēr nav labi pārdomāta attiecīga resursu piešķīruma. Ir pieņemts maz kompromisa lēmumu par "relatīvajiem" ieguldījumiem dažādajos aspekta elementos. Tomēr aspekts ir funkcionāls un noteikts;
- **stratēģiskais posms**. Ir izdarītas izvēles attiecībā uz to, kuras aspekta daļas konkrētajai organizācijai vai valstij ir svarīgas un kuras ir mazāk svarīgas. Stratēģiskais posms atspoguļo to, ka šīs izvēles ir izdarītas saskaņā ar valsts vai organizācijas konkrētajiem apstākļiem;
- **dinamiskais posms**. Šajā posmā ir ieviesti skaidri mehānismi stratēģijas mainīšanai atkarībā no valdošajiem apstākļiem, piem., apdraudējumu vides tehnoloģijām, konfliktiem pasaulē vai būtiskām pārmaiņām kādā problēmjomā (piem., kibernoziedzības vai privātuma jomā). Dinamiskām organizācijām ir labi izstrādātas metodes plūdenai izmaiņu ieviešanai stratēģijās. Šim posmam raksturīga ātra lēmumu pieņemšana, resursu pārdalīšana un nepārtrauktas uzmanības pievēršana mainīgajai videi.

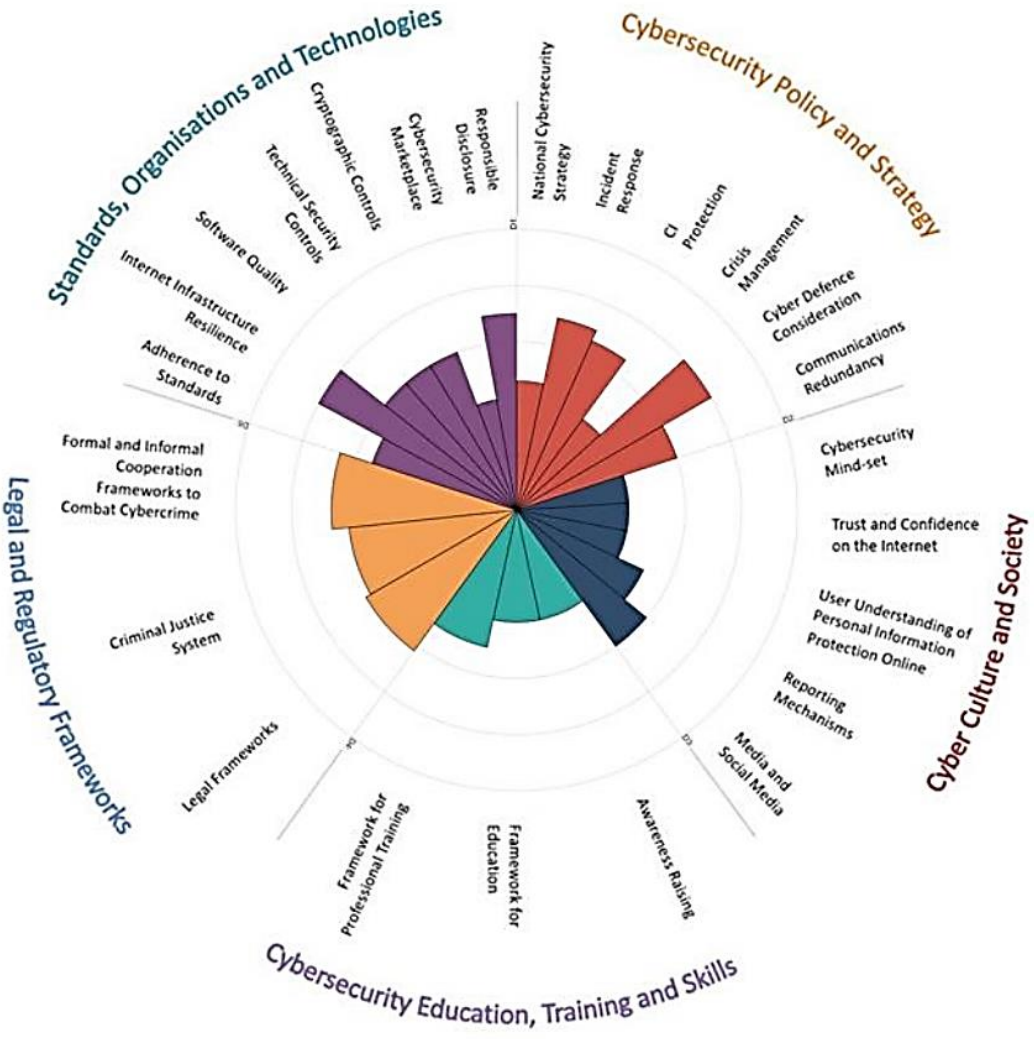
Novērtēšanas metode

Tā kā Spēju centram nav pilnīgas un padziļinātas izpratnes par katras valsts vietējiem apstākļiem, kuros attiecīgais modelis tiek izmantots, tas kiberdrošības spēju gatavības pārskatīšanā sadarbojas ar starptautiskām organizācijām un uzņēmējām ministrijām vai organizācijām attiecīgajā valstī. Lai novērtētu *CMM* iekļauto piecu virzienu gatavības līmeni, Spēju centrs un uzņēmēja organizācija divas vai trīs dienas tiekas ar attiecīgām valsts publiskā un privātā sektora ieinteresētajām personām fokusgrupās, kurās tiek aplūkoti *CMM* virzieni. Katru virzienu pārrunā vismaz divas reizes dažādās ieinteresēto personu grupās. Tā tiek iegūts sākotnējo datu kopums, kas pēc tam tiek izmantots novērtēšanā.

Rezultātu veids vai atspoguļojums

CMM sniedz pārskatu par katras valsts gatavības līmeni, izmantojot radardiagrammu ar pieciem sektoriem — vienu katram virzienam. Katrs virziens aizņem vienu piekto daļu diagrammas, un katra faktora piecas gatavības pakāpes sniedzas no diagrammas centra uz āru; kā redzams zemāk, sākumposms ir vistuvāk diagrammas centram, bet dinamiskais posms ir pie ārmalas.

5. attēls. *CMM*: rezultātu pārskats



Standards, Organisations and Technologies	Standarti, organizācijas un tehnoloģijas
Legal Regulatory Frameworks	Tiesiskais un normatīvais regulējums
Cybersecurity Education, Training and Skills	Kiberdrošības izglītība, apmācība un prasmes
Cybersecurity Policy and Strategy	Kiberdrošības politika un stratēģija
Cyber Culture and Society	Kiberdrošības kultūra un sabiedrība
Responsible Disclosure	Atbildīga atklāšana
Cybersecurity market place	Kiberdrošības tirgus
Technical Security Controls	Tehniskās drošības kotrole
Cryptographic Controls	Kriptogrāfiskās kontroles
Software Quality	Programmatūras kvalitāte
Internet Infrastructure Resilience	Interneta infrastruktūras noturība
Adherence to Standards	Standartu ievērošana
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formālas un neformālas sadarbības sistēmas kibernoziedzības apkarošanai
Criminal Justice System	Krimināltiesību sistēma
Legal Frameworks	Tiesiskais regulējums
Framework for Professional Training	Profesionālās apmācības satvars
Framework for Education	Izglītības satvars
Awareness Raising	Izpratnes vairošana

Media and Social Medai	Sociālie un citi plašsaziņas līdzekļi
Reporting Mechanisms	Ziņošanas mehānismi
User Understanding of Personal Information Protection Online	Lietotāju izpratne par persondatu aizsardzību tiešsaistē
Trust and Confidence on the Internet	Uzticība un pārliecība internetā
Cybersecurity Mind-set	Uz kiberdrošību vērsta domāšana
Communications Redundancy	Sakaru redundance
Cyber Defence Consideration	Kiberaizsardzības apsvērumi
Crisis Management	Krīžu pārvarēšana
CI Protection	Krit. infr. aizsardzība
Incident Response	Reaģēšana uz incidentiem
National Cybersecurity Strategy	Valsts kiberdrošības stratēģija

Globālais kiberdrošības spēju centrs, Oksfordas Mārtina skola, Oksfordas Universitāte, 2017.

A.2 Kiberdrošības spēju gatavības modelis (*C2M2*)

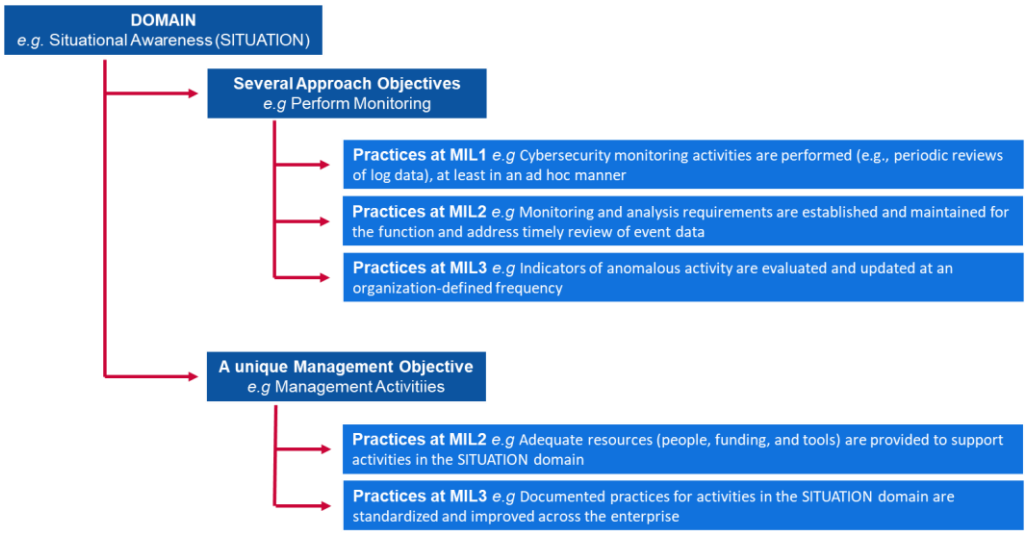
Kiberdrošības spēju gatavības modeli (*C2M2*) ir izstrādājis ASV Enerģētikas departaments sadarbībā ar privātā un publiskā sektora ekspertiem. Spēju centra mērķis ir palīdzēt visu nozaru, veidu un lielumu organizācijām izvērtēt savas kiberdrošības programmas, tās uzlabot un nostiprināt savu darbības noturību. *C2M2* galvenā uzmanība ir pievērsta tās kiberdrošības prakses īstenošanai un pārvaldībai, kura ir saistīta ar informācijas, informācijas tehnoloģiju (IT) un operāciju tehnoloģiju (OT) līdzekļiem un to darbības vidi. Gatavības modeļi *C2M2* ir definēti kā "īpašību, atribūtu, rādītāju vai darbības modeļu kopa, kas atspoguļo spējas un virzību konkrētā disciplīnā". *C2M2* pirmoreiz tika ieviests 2014. gadā, bet 2019. gadā tas tika pārskatīts.

Atribūti/virzieni

C2M2 ir aplūkotas **10 jomas**, kurās ir loģiski sagrupētas kiberdrošības prakses. Katrs prakšu kopums ietver pasākumus, ko organizācija var īstenot, lai izveidotu un nostiprinātu spējas konkrētajā jomā. Katra joma ir saistīta ar **vienu pārvaldības mērķi** un **vairākiem pieejas mērķiem**. Gan pieejas, gan pārvaldības mērķos ir izklāstītas **vairākas prakses**, kas apraksta institucionalizētas darbības.

Attiecības starp šiem jēdzieniem ir īsumā parādītas tālāk.

6. attēls. *C2M2* rādītāja piemērs



Domain eg Situational Awareness (SITUATION)	**Joma**, piem., situācijas apzināšanās (SITUĀCIJA)
Several Approaches Objectives e.g. Perform Monitoring	**Vairāki pieejas mērķi**, piem., veikt uzraudzību
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**1. GRL prakses**, piem., tiek veiktas kiberdrošības uzraudzības darbības (piem., tiek periodiski pārskatīti žurnāla dati), vismaz pēc vajadzības
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**2. GRL prakses**, piem., ir noteiktas un tiek uzturētas attiecīgās funkcijas uzraudzības un analīzes prasības, kas nodrošina, ka notikuma dati tiek laikus pārskatīti
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**3. GRL prakses**, piem., organizācijas noteiktā biežumā tiek izvērtēti un atjaunināti netipisku darbību rādītāji
A unique Management Objectve e.g. Management Activities	**Viens pārvaldības mērķis**, piem., pārvaldības darbības
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**2. GRL prakses**, piem., ir nodrošināti pietiekami resursi (cilvēki, finansējums un rīki) SITUĀCIJAS jomas darbību atbalstam
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**3. GRL prakses**, piem., visā uzņēmumā tiek izmantotas standartizētas, dokumentētas prakses, kas attiecas uz SITUĀCIJAS jomas darbībām, un tās tiek uzlabotas

10 minētās jomas ir šādas:

i riska pārvaldība (RISKS);
ii līdzekļu, pārmaiņu un konfigurācijas pārvaldība (LĪDZEKĻI);
iii identitātes un piekļuves pārvaldība (PIEKĻUVE);
iv apdraudējumu un ievainojamību pārvaldība (DRAUDI);
v situācijas apzināšanās (SITUĀCIJA);
vi reaģēšana uz notikumiem un incidentiem (REAKCIJA);
vii piegādes ķēdes un ārējo atkarību pārvaldība (ATKARĪBA);
viii darbaspēka pārvaldība (DARBASPĒKS);
ix kiberdrošības arhitektūra (ARHITEKTŪRA);
x kiberdrošības programmas pārvaldība (PROGRAMMA).

Gatavības līmeņi

C2M2 izmanto **četrus gatavības līmeņus** (tos dēvē par gatavības rādītāju līmeņiem — GRL), kas atspoguļo gatavības progresu divos aspektos — pieejas progresu un pārvaldības progresu. GRL ir numurēti no 0. GRL līdz 3. GRL, un tos ir paredzēts piemērot neatkarīgi katrai jomai.

- **0. GRL**: nekāda prakse netiek īstenota.
- **1. GRL**: tiek īstenota sākotnēja prakse, bet, iespējams, tikai pēc vajadzības.
- **2. GRL**: pārvaldības raksturojums:
  - prakse tiek dokumentēta;
  - procesa atbalstam ir nodrošināti pietiekami resursi;
  - personālam, kas īsteno praksi, ir atbilstošas prasmes un zināšanas;
  - atbildība par prakses īstenošanu un ar prakses īstenošanu saistītās pilnvaras ir piešķirtas konkrētam dalībniekam;

  pieejas raksturojums:
  - prakse ir pilnīgāka vai augstāk attīstīta nekā 1. GRL.
- **3. GRL**: pārvaldības raksturojums:
  - darbības tiek īstenotas saskaņā ar politiku (vai citiem organizācijas norādījumiem);
  - ir noteikti un tiek uzraudzīti jomas darbību rezultātu mērķi, lai sekotu līdzi sasniegumiem;
  - visā uzņēmumā tiek izmantotas standartizētas, dokumentētas prakses, kas attiecas uz jomas darbībām, un tās tiek uzlabotas;

  pieejas raksturojums:
  - prakse ir pilnīgāka vai augstāk attīstīta nekā 2. GRL.

Novērtēšanas metode

Ir paredzēts, ka organizācija izmanto *C2M2* kopā ar **pašizvērtēšanas metodiku** un rīkkopu (pieejamas pēc pieprasījuma), lai novērtētu un uzlabotu savu kiberdrošības programmu. Pašizvērtējumu ar rīkkopu var pabeigt vienā dienā, bet rīkkopu varētu pielāgot, lai varētu iegūt rūpīgāku izvērtējumu. *C2M2* var izmantot arī, lai gūtu informāciju, uz kuras pamata var izstrādāt jaunu kiberdrošības programmu.

Modeļa saturs ir izklāstīts ļoti vispārīgi, tāpēc dažādu veidu, struktūru, lielumu un nozaru organizācijas to var interpretēt pēc sava prāta. Ja nozarē modeli izmanto plaši, pieaug nozares

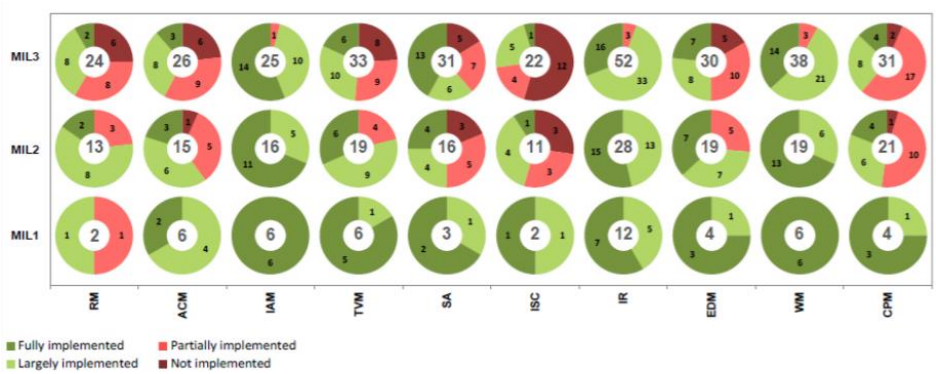
dalībnieku iespējas savas kiberdrošības spējas salīdzināt ar citu nozares dalībnieku kiberdrošības spējām.

Rezultātu veids vai atspoguļojums

C2M2 uz aptaujas rezultātu pamata ģenerē pārskatu par izvērtējumā iegūto vērtējumu. Šajā pārskatā rezultāti ir atspoguļoti divos skatos: mērķu skatā, kurā ir parādītas atbildes uz prakses jautājumiem sadalījumā pa jomām un to mērķiem, un jomu skatā, kurā ir parādītas atbildes visās jomās un GRL. Abu līmeņu atspoguļošanai tiek izmantota attēlošanas sistēma ar sektoru diagrammām (viena diagramma katrai atbildei) un luksofora sistēma kā vērtējuma piešķiršanas mehānisms. Kā redzams 7. , sektoru diagrammas sarkanie sektori parāda, uz cik daudziem aptaujas jautājumiem tika atbildēts ar "nav īstenots" (tumši sarkans) vai "daļēji īstenots" (gaiši sarkans). Zaļie sektori parāda, uz cik daudziem jautājumiem tika atbildēts ar "lielā mērā īstenots" (gaiši zaļš) vai "pilnīgi īstenots" (tumši zaļš).

7. ir piemērs rādītāju sistēmai, kas tiek iegūta gatavības novērtējuma beigās. Uz X ass ir *C2M2* 10 jomas, bet uz Y ass — gatavības līmeņi (GRL). Ja diagrammā aplūko riska pārvaldības (RP) jomu, var redzēt trīs sektoru diagrammas — pa vienai katrā gatavības līmenī (1. GRL, 2. GRL un 3. GRL). Diagrammā ir redzams, ka RP jomā ir jāizvērtē divi jautājumi, lai sasniegtu pirmo gatavības līmenī (1. GRL). Šajā gadījumā viens saņēma vērtējumu "lielā mērā īstenots", bet otrs — "daļēji īstenots". Modelī ir paredzēts, ka otrajā gatavības līmenī (2. GRL) ir jāizvērtē 13 jautājumi. Divi no šiem 13 jautājumiem attiecas uz pirmo līmeni (1. GRL), bet 11 uz otro līmeni (2. GRL). Tādu pašu principu piemēro arī trešajā līmenī (3. GRL).

7. attēls. *C2M2* — jomu skata piemērs



Fully implemented	Pilnīgi īstenots
Largely implemented	Lielā mērā īstenots
Partially implemented	Daļēji īstenots
Not implemented	Nav īstenots
MIL1	1. GRL
MIL2	2. GRL
MIL3	3. GRL
RM	RP
ACM	LPKP
IAM	IPP
TVM	AIP
SA	SA
ISC	IKK
IR	RNI
EDM	ĀAP
WM	DP
CPM	KPP

Avots: ASV Enerģētikas departaments, Elektroenerģijas piegādes un enerģijas uzticamības birojs, 2015.

A.3 Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēma

Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēmu izstrādāja Standartu un tehnoloģiju valsts institūtā (*NIST*). Tās mērķis ir virzīt kiberdrošības darbības un pārvaldīt riskus organizācijā. Tā ir paredzēta visu veidu organizācijām neatkarīgi no to lieluma, kiberdrošības riska pakāpes un kiberdrošības attīstības pakāpes. Tā kā šī ir sistēma, nevis modelis, tā ir strukturēta citādi nekā iepriekš analizētie modeļi.

Sistēmai ir trīs daļas: sistēmas kodols, īstenošanas līmeņi un sistēmas profili.

- **Sistēmas kodolā** ir apkopoti kiberdrošības pasākumi, vēlamie iznākumi un piemērojamās atsauces, ko bieži izmanto kritiskās infrastruktūras nozarēs. Tie ir līdzīgi kiberdrošības spēju gatavības modeļos iekļautajiem atribūtiem vai virzieniem.
- **Sistēmas īstenošanas līmeņi** (tālāk "līmeņi") sniedz pārskatu par to, kā organizācija uztver kiberdrošības risku un šā riska pārvaldības nolūkā ieviestos procesus. Viszemākais līmenis ir "daļējais" (1. līmenis), bet visaugstākais — "adaptīvais" (4. līmenis), un, jo augstāks līmenis, jo kiberdrošības riska pārvaldības prakses ir rūpīgāk izstrādātas un izkoptākas. Līmeņi neatspoguļo gatavības līmeņus, tie drīzāk palīdz pieņemt organizatoriskus lēmumus par to, kā pārvaldīt kiberdrošības risku un kuri organizācijas aspekti ir uzskatāmi par prioritāri nozīmīgākiem un varētu saņemt papildu resursus.
- **Sistēmas profils** (tālāk "profils") atspoguļo iznākumus, pamatojoties uz darbības vajadzībām, ko organizācija ir atlasījusi no sistēmas kategorijām un apakškategorijām. Profilu var raksturot attiecībā uz standartu, pamatnostādņu un prakšu saskaņotību ar sistēmas kodolu konkrētā īstenošanas scenārijā. Profilus var izmantot, lai, salīdzinot "pašreizējo" profilu (pašreizējo stāvokli) ar "mērķa" profilu (stāvokli, kādam tam jābūt), noteiktu, kādas ir iespējas uzlabot kiberdrošības stāvokli.

Sistēmas kodols

Sistēmas kodols sastāv no piecām **funkcijām**. Aplūkotas kopā, šīs funkcijas sniedz vispārīgu, stratēģisku pārskatu par organizācijas kiberdrošības riska pārvaldības dzīves ciklu. Sistēmas kodolā katrai funkcijai ir noteiktas tās pamatā esošās galvenās **kategorijas** un **apakškategorijas**, un katra apakškategorija ir sasaistīta ar informatīvu atsauču piemēriem, tādiem kā spēkā esoši standarti, pamatnostādnes un prakse.

Funkcijas un kategorijas ir sīkāk iztirzātas tālāk.

i **Noteikt**: radīt organizācijā izpratni par to, kā pārvaldīt kiberdrošības riskus, kas skar sistēmas, cilvēkus, līdzekļus, datus un spējas.
   - Apakškategorijas: līdzekļu pārvaldība; darbības vide; pārvaldība; riska novērtēšana; riska pārvaldības stratēģija.

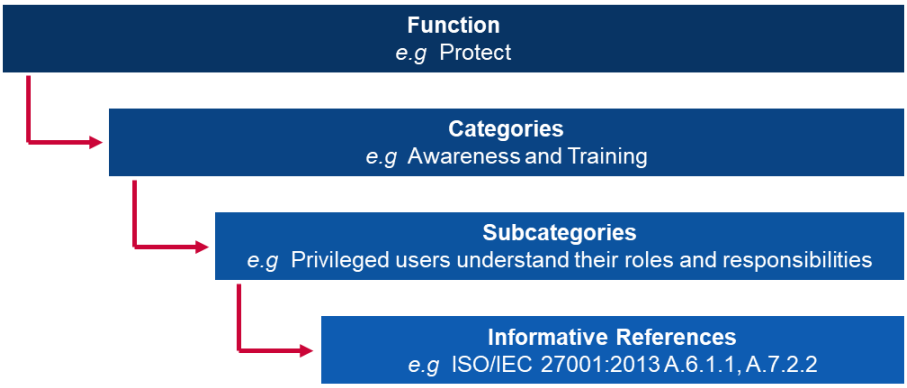
ii **Aizsargāt**: izstrādāt un ieviest pienācīgus aizsardzības pasākumus, lai nodrošinātu kritisko pakalpojumu sniegšanu.
   - Apakškategorijas: identitātes pārvaldība un piekļuves kontrole; apzināšanās un apmācība; datu drošība; informācijas aizsardzības procesi un procedūras; uzturēšana; aizsardzības tehnoloģijas.

iii **Atklāt**: izstrādāt un īstenot atbilstošas darbības, lai noteiktu, ka ir atgadījies kiberdrošības notikums.
   - Apakškategorijas: anomālijas un notikumi; nepārtraukta drošības uzraudzība; atklāšanas procesi.

iv **Reaģēt**: izstrādāt un īstenot atbilstošas darbības, kas jāveic, ja ir atklāts kiberdrošības incidents.
   - Apakškategorijas: reaģēšanas plānošana; sakari; analīze; seku mazināšana; uzlabojumi.

- **Atkopt**: izstrādāt un īstenot atbilstošas darbības, kas jāveic, lai uzturētu noturības plānus un atjaunotu spējas vai pakalpojumus, kas tikuši skarti kiberdrošības incidentā.
  - Apakškategorijas: atkopšanas plānošana; uzlabojumi; sakari.

8. attēls. Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēmas piemērs



Function e.g Project	**Funkcija**, piem., aizsargāt
Categories e.g Awarness and Training	**Kategorijas**, piem., apzināšanās un apmācība
Subcategories e.g Privileged useres understand their roles and responsibilities	**Apakškategorijas**, piem., privileģēti lietotāji apzinās savu lomu un pienākumus
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informatīvas atsauces**, piem., ISO/IEC 27001:2013, A.6.1.1., A.7.2.2.

Līmeņi

Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēmai ir **četri līmeņi**, un katrs no tiem ir noteikts trīs aspektos: riska pārvaldības process, integrētas riska pārvaldības programma un ārējā dalība. Šie līmeņi jāuzskata nevis par gatavības līmeņiem, bet gan par satvaru, kas sniedz pārskatu par to, kā organizācijas uztver kiberdrošības risku un šā riska pārvaldības nolūkā ieviestos procesus.

- **1. līmenis: daļējais**
  - **Riska pārvaldības process**: organizatoriskā kiberdrošības riska pārvaldības prakse nav formalizēta, un risku pārvalda pēc nepieciešamības un — dažkārt — reaģējot uz notikumiem.
  - **Integrētas riska pārvaldības programma**: organizācija maz apzinās kiberdrošības risku. Organizācija pārvalda kiberdrošības risku neregulāri, atsevišķos gadījumos, un tai var nebūt procesu, kas dod iespēju dalīties ar kiberdrošības informāciju organizācijas iekšienē.
  - **Ārēja dalība**: organizācija nesaprot savu lomu plašākā ekosistēmā ne attiecībā uz tās atkarību no citiem, ne attiecībā uz citu atkarību no tās. Organizācija kopumā neapzinās tās nodrošināto un izmantoto produktu un pakalpojumu piegādes ķēdes kiberdrošības riskus.
- **2. līmenis: informēts par risku**
  - **Riska pārvaldības process**: vadība ir apstiprinājusi riska pārvaldības praksi, bet tā var nebūt ieviesta kā politika visas organizācijas mērogā.
  - **Integrētas riska pārvaldības programma**: organizācija apzinās kiberdrošības risku, bet nav ieviesta organizācijas mēroga pieeja kiberdrošības riska pārvaldībai. Organizācijas un ārējo līdzekļu kiberdrošības risks tiek novērtēts, bet parasti šo novērtējumu nevar atkārtot un tas netiek veikts regulāri.
  - **Ārēja dalība**: organizācija kopumā saprot savu lomu plašākā ekosistēmā vai nu attiecībā uz tās atkarību no citiem, vai arī attiecībā uz citu atkarību no tās, bet ne uz abu veidu atkarību. Organizācija arī apzinās piegādes ķēdes kiberdrošības riskus, kas ir saistīti ar tās nodrošinātajiem un izmantotajiem produktiem un pakalpojumiem, bet tā pret šiem riskiem nevēršas konsekventi vai oficiāli.

- **3. līmenis: atkārtojams**
  - **Riska pārvaldības process**: organizācijas riska pārvaldības prakse ir oficiāli apstiprināta un izveidota politikas formā. Organizācijas kiberdrošības prakse tiek regulāri atjaunināta, pamatojoties uz riska pārvaldības procesu piemērošanu izmaiņām darbības/misijas prasībās un mainīgajai apdraudējumu un tehnoloģiju ainai.
  - **Integrētas riska pārvaldības programma**: ir kiberdrošības riska pārvaldības pieeja, kas tiek izmantota visā organizācijā. Tiek noteikta, saskaņā ar iecerēm īstenota un pārskatīta informācijā par risku balstīta politika, procesi un procedūras. Augstākā līmeņa vadošie darbinieki nodrošina, ka kiberdrošības apsvērumi tiek ņemti vērā visos organizācijas darbības virzienos.
  - **Ārēja dalība**: organizācija saprot savu lomu plašākā ekosistēmā, savu atkarību no citiem un citu atkarību no tās un var veicināt risku izpratnes paaugstināšanos kopienā. Organizācija apzinās piegādes ķēdes kiberdrošības riskus, kas ir saistīti ar tās nodrošinātajiem un izmantotajiem produktiem un pakalpojumiem.
- **4. līmenis: adaptīvais**
  - **Riska pārvaldības process**: organizācija pielāgo savu kiberdrošības praksi, pamatojoties uz iepriekšējām un pašreizējām kiberdrošības darbībām, ņemot vērā arī gūtās mācības un prognostiskos rādītājus.
  - **Integrētas riska pārvaldības programma**: visā organizācijā tiek izmantota kiberdrošības riska pārvaldības pieeja, kuras ietvaros tiek izmantota uz riska informāciju balstīta politika, procesi un procedūras, lai nodrošinātos pret iespējamiem kiberdrošības notikumiem.
  - **Ārēja dalība**: organizācija saprot savu lomu plašākā ekosistēmā, savu atkarību no citiem un citu atkarību no tās un veicina risku izpratnes paaugstināšanos kopienā.

Novērtēšanas metode

Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēmas mērķis ir dot organizācijām iespēju pašām novērtēt savu risku, lai varētu padarīt savu kiberdrošības pieeju un ieguldījumus racionālākus, efektīvākus un vērtīgākus. Lai pārbaudītu ieguldījumu efektivitāti, organizācijai vispirms ir skaidri jāsaprot, kādi ir tās kā organizācijas mērķi un kādas ir attiecības starp šiem mērķiem un tos sekmējošiem kiberdrošības iznākumiem. Sistēmas kodola kiberdrošības iznākumi palīdz veikt ieguldījumu efektivitātes un kiberdrošības pasākumu pašnovērtējumu.

A.4 Kataras kiberdrošības spēju gatavības modelis (*Q-C2M2*)

Kataras kiberdrošības spēju gatavības modeli (*Q-C2M2*) izstrādāja Kataras Universitātes Jurisprudences koledža 2018. gadā. *Q-C2M2* izveidē tika izmantoti dažādi jau pastāvoši modeļi, lai izstrādātu visaptverošu novērtēšanas metodiku, ar ko varētu uzlabot Kataras kiberdrošības satvaru.

Atribūti/virzieni

Q-C2M2 tiek izmantota Standartu un tehnoloģiju valsts institūta (*NIST*) sistēmas pieeja, kurā par modeļa galvenajām jomām tiek pieņemtas piecas pamatfunkcijas. Kataras apstākļiem šīs piecas pamatfunkcijas der, jo tās ir kopīgas visām kritiskās infrastruktūras nozarēm, kas ir būtisks Kataras kiberdrošības satvara elements. *Q-C2M2* ir **piecas jomas**, un katra joma ir sadalīta vairākās **apakšjomās**, lai aptvertu visu kiberdrošības spēju gatavības loku.

Piecas minētās jomas ir šādas:

i **izpratnes joma** ar šādām četrām apakšjomām: kiberpārvaldība, līdzekļi, riski un apmācība;
ii **drošības joma** ar šādām apakšjomām: datu drošība, tehnoloģiju drošība, piekļuves kontroles drošība, sakaru drošība un personāla drošība;
iii **riska ietekmes joma** ar šādām apakšjomām: uzraudzība, incidentu pārvaldība, atklāšana, analīze un riska ietekme;
iv **reaģēšanas joma** ar šādām apakšjomām: reaģēšanas plānošana, ietekmes mazināšana un saziņa reaģēšanas kontekstā;

- **stiprināšanas joma** ar šādām apakšjomām: atkopšanas plānošana, nepārtrauktības pārvaldība, uzlabošana un ārēja atkarība.

Gatavības līmeņi

Q-C2M2 ir **pieci gatavības līmeņi**, kas atspoguļo valsts struktūras vai nevalstiskas organizācijas spēju gatavību pamatfunkciju līmenī. Ar šiem līmeņiem ir paredzēts novērtēt gatavību piecās jomās, kas ir aprakstītas iepriekšējā iedaļā.

- **Sākuma**: izmanto *ad hoc* kiberdrošības prakses un procesus dažās jomās.
- **Ieviešanas**: ir pieņemta politika, kurā paredzēts līdz noteiktam laikam īstenot visas jomās noteiktās kiberdrošības darbības.
- **Attīstības**: tiek īstenota politika un prakse jomās noteikto kiberdrošības darbību attīstīšanai un uzlabošanai ar mērķi ieteikt jaunas īstenojamas darbības.
- **Adaptīvais**: tiek atkārtoti aplūkotas un pārskatītas kiberdrošības darbības un pieņemta prakse, pamatojoties uz prognostiskajiem rādītājiem, kas izriet no iepriekšējās pieredzes un pasākumiem.
- **Ātrdarbības**: tiek turpināts adaptīvajā posmā aprakstītais, bet lielāks uzsvars tiek likts uz ātru reakciju un ātrumu darbību īstenošanā jomās.

Novērtēšanas metode

Q-C2M2 ir sākotnējā izpētes posmā un vēl nav gatavs ieviešanai. Tas ir satvars, ko nākotnē varētu izmantot, lai ieviestu detalizētas novērtēšanas modeli Kataras organizācijām.

A.5 Kiberdrošības gatavības modeļa sertifikācija (*CMMC*)

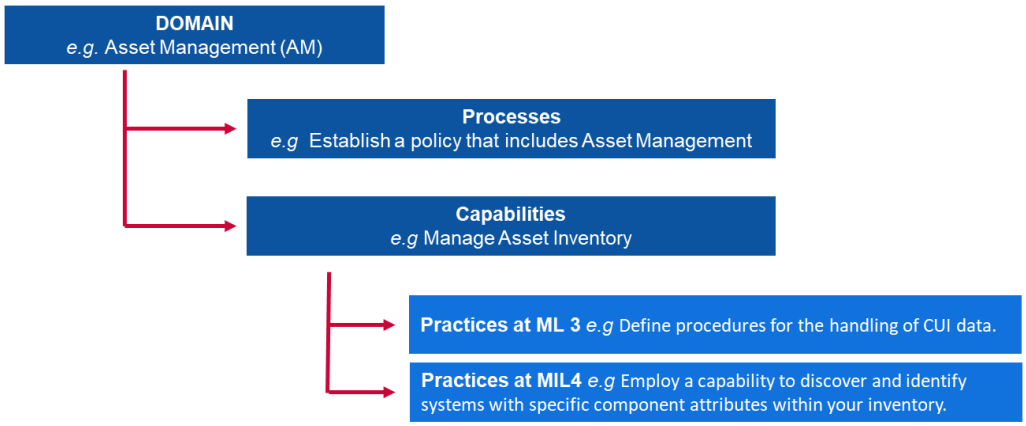
Kiberdrošības gatavības modeļa sertifikāciju (*CMMC*) ir izstrādājis ASV Aizsardzības departaments sadarbībā ar Kārnegija un Melona universitāti un Džona Hopkinsa universitātes Lietišķās fizikas laboratoriju. Aizsardzības departamenta galvenais mērķis šā modeļa izstrādē bija aizsargāt aizsardzības rūpnieciskā pamata sektora informāciju. Informācija, uz ko attiecas *CMMC*, ir klasificēta kā "federālo līgumu informācija", proti, informācija, ko sniedz valdība vai kas ir radīta valdības vajadzībām saskaņā ar līgumu un ko nav paredzēts publiskot, vai kā "kontrolēta neklasificēta informācija", proti, informācija, kura jāaizsargā vai kuras izplatīšana jākontrolē, pamatojoties uz un saskaņā ar normatīvajiem aktiem un valdības līmeņa politiku. *CMMC* novērtē kiberdrošības gatavību un sniedz paraugpraksi, turklāt tam ir arī sertifikācijas elements, kura mērķis ir nodrošināt, ka ar katru gatavības līmeni saistītā prakse tiek reāli īstenota. *CMMC* jaunākā versija tika izlaista 2020. gadā.

Atribūti/virzieni

CMMC ir aplūkotas **17 jomas**, kas ir kiberdrošības procesu un spēju grupas. Katra joma ir iedalīta sīkāk vairākos **procesos**, kas visās jomās ir līdzīgi, un vienā, vairākās vai daudzās **spējās**, kas ir sadalītas pa pieciem gatavības līmeņiem. Spējas (vai spēja) ir sīkāk sadalīta(-as) **praksēs** katram attiecīgajam gatavības līmenim.

Attiecības starp šiem jēdzieniem ir atspoguļotas nākamajā attēlā.

9. attēls. *CMMC* rādītāju piemērs



DOMAIN e.g. Asset Management (AM)	**JOMA**, piem., līdzekļu pārvaldība (LP)
Processes e.g Establish a policy that includes Asset Management	**Procesi**, piem., izveidot politiku, kas ietver līdzekļu pārvaldību
Capabilities e.g Manage Asset Inventory	**Spējas**, piem., pārvaldīt līdzekļu krājumu
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Prakses 3. GL**, piem., noteikt procedūras KNI datu apstrādei
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Prakses 4. GL**, piem., izmantot spēju atklāt un identificēt inventārā sistēmas, kuras ietver konkrētus atribūtus

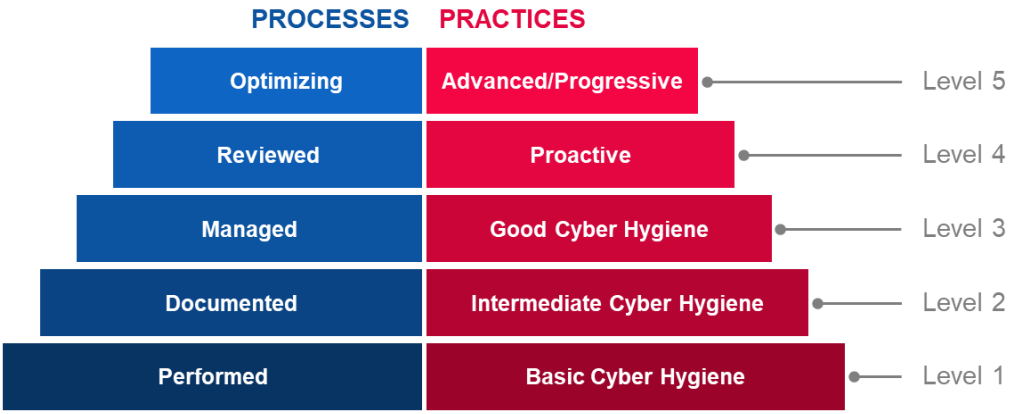
17 minētās jomas ir šādas:

i piekļuves kontrole (PK);
ii līdzekļu pārvaldība (LP);
iii revīzija un pārskatatbildība (RP);
iv apzināšanās un apmācība (AA);
v konfigurācijas pārvaldība (KP);
vi identificēšana un autentificēšana (IA);
vii reaģēšana uz incidentiem (RI);
viii uzturēšana (U);
ix informācijas nesēju aizsardzība (INA);
x personāla drošība (PD);
xi fiziskā aizsardzība (FA);
xii atkopšana (A);
xiii riska pārvaldība (RiP);
xiv drošības novērtēšana (DN);
xv situācijas apzināšanās (SA);
xvi sistēmu un sakaru aizsardzība (SSA);
xvii sistēmu un informācijas integritāte (SII).

Gatavības līmeņi

CMMC ir **pieci gatavības līmeņi**, kas noteikti, pamatojoties uz procesiem un praksēm. Lai Kiberdrošības gatavības modeļa sertifikācijā sasniegtu noteiktu gatavības līmeni, organizācijai ir jāizpilda konkrētā līmeņa procesu un prakšu priekšnoteikumi. Tas turklāt nozīmē, ka ir jāizpilda arī visu zemāko līmeņu priekšnoteikumi.

10. attēls. *CMMC* gatavības līmeņi



PROCESSES	PROCESI
Optimizing	Tiek optimizēti
Reviewed	Tiek pārskatīti
Managed	Tiek pārvaldīti
Documented	Ir dokumentēti
Performed	Tiek īstenoti:
PRACTICES	PRAKSES
Advanced/Progressive	Augsti attīstītas / progresīvas
Proactive	Proaktīvas
Good Cyber Hygiene	Laba kiberhigiēna
Intermediate Cyber Hygiene	Viduvēja kiberhigiēna
Basic Cyber Hygiene	Pamata kiberhigiēna
Level 5	5. līmenis
Level 4	4. līmenis
Level 3	3. līmenis
Level 2	2. līmenis
Level 1	1. līmenis

- **1. līmenis**
  - **Procesi — tiek īstenoti**: organizācija, iespējams, spēj īstenot šīs prakses tikai tad, kad nepieciešams, un tās var būt vai nebūt dokumentētas. Procesu gatavība 1. līmenī netiek novērtēta.
  - **Prakses — pamata kiberhigiēna**: 1. līmenī galvenā uzmanība tiek pievērsta FLI (federālo līgumu informācijas) aizsardzībai, un tas ietver tikai tādas prakses, kas atbilst pamata aizsardzības nodrošināšanas prasībām.
- **2. līmenis**
  - **Procesi — ir dokumentēti**: 2. līmenī organizācijai jābūt izveidotām un dokumentētām praksēm un politikai, kas virza tās *CMMC* centienu īstenošanu. Ja prakses ir dokumentētas, personas tās var īstenot atkārtoti. Organizācijas panāk spēju gatavību, dokumentējot savus procesus un tad tos īstenojot tā, kā norādīts dokumentos.
  - **Prakses — viduvēja kiberhigiēna**: 2. līmenis ir pārejas posms no 1. līmeņa uz 3. līmeni un ietver daļu no NIST SP 800-171 noteiktajām drošības prasībām, kā arī prakses no citiem standartiem un atsauces dokumentiem.
- **3. līmenis**

- **Procesi — tiek pārvaldīti**: 3. līmenī organizācijai jāizveido, jāuztur un jāapgādā ar resursiem plāns, kas parāda, kā tiek pārvaldītas prakses īstenošanai nepieciešamās darbības. Plānā var būt iekļauta informācija par uzdevumiem, mērķiem, projektu plāniem, resursiem, nepieciešamo apmācību un attiecīgu ieinteresēto personu iesaisti.
- **Prakses — laba kiberhigiēna**: 3. līmenī uzmanība tiek pievērsta KNI (kontrolētas neklasificētas informācijas) aizsardzībai, un tajā ir ietvertas visas NIST SP 800-171 noteiktās drošības prasības, kā arī papildu prakses no citiem standartiem un atsauces dokumentiem, lai mazinātu apdraudējumu ietekmi.

4. līmenis

- **Procesi — tiek pārskatīti**: 4. līmenī organizācijai jāpārskata prakses un jāvērtē to efektivitāte. Organizācijas šajā līmenī ne tikai vērtē prakšu efektivitāti, bet arī var nepieciešamības gadījumā veikt korektīvas darbības un regulāri informēt augstākā līmeņa vadību par stāvokli vai problēmām.
- **Prakses — proaktīvas**: 4. līmenī galvenā uzmanība tiek pievērsta KNI aizsardzībai, un tajā ir ietverta daļa no pastiprinātajām drošības prasībām. Šīs prakses uzlabo organizācijas atklāšanas un reaģēšanas spējas, lai tā varētu labāk tikt galā ar mainīgajām taktikām, paņēmieniem un procedūrām un pielāgoties tām.

5. līmenis

- **Procesi — tiek optimizēti**: 5. līmenī organizācijai ir jāstandartizē un jāoptimizē procesu īstenošana visā organizācijā.
- **Prakses — augsti attīstītas / proaktīvas**: 5. līmenī galvenā uzmanība tiek pievērsta KNI aizsardzībai. Papildu prakses padziļina un izkopj kiberdrošības spējas.

Novērtēšanas metode

CMMC ir salīdzinoši jauns modelis, kas tika pabeigts 2020. gada pirmajā ceturksnī. Līdz šim to nav izmantojusi neviena organizācija. Tomēr Aizsardzības departamenta darbuzņēmēji plāno uzrunāt sertificētus ārējus pārbaudītājus, lai tie veiktu revīzijas. Aizsardzības departaments sagaida, ka tā darbuzņēmēji īstenos paraugpraksi, lai paaugstinātu kiberdrošību un sensitīvas informācijas aizsardzību.

A.6 Pašvaldību kiberdrošības gatavības modelis (*CCSMM*)

Pašvaldību kiberdrošības gatavības modeli (*CCSMM*) ir izstrādājis Teksasas Universitātes Infrastruktūras aizsardzības un drošības centrs. *CCSMM* mērķis ir labāk noteikt metodes, kā konstatēt, cik lielā mērā pašvaldība pašlaik ir sagatavota kiberdrošības jomā, un nodrošināt ceļvedi, ko pašvaldības var izmantot par atsauci savos sagatavošanās centienos. Pašvaldības, kam *CCSMM* galvenokārt ir paredzēts, ir vietējās vai štata pašvaldības. *CCSMM* tika izstrādāts 2007. gadā.

Atribūti/virzieni

Gatavības līmeņi ir noteikti **sešos galvenajos virzienos**, kas aptver dažādus pašvaldību un organizāciju kiberdrošības aspektus. Šie virzieni ir skaidri definēti katram gatavības līmenim (sīkāk izklāstīti 31.attēlā Kopsavilkums par CCSMM"). Seši minētie virzieni ir šādi:

i novēršamie draudi;
ii rādītāji;
iii informācijas kopīgošana;
iv tehnoloģijas;
v apmācība;
vi testēšana.

Gatavības līmeņi

CCSMM ir iedalīts **piecos gatavības līmeņos**, un katram līmenim ir raksturīgi savi galvenie apdraudējumu un darbību veidi.

- **1. līmenis: drošības apzināšanās**
  Šā līmeņa pasākumu galvenais mērķis ir likt personām un organizācijām apzināties draudus, problēmas un problēmjautājumus, kas saistīti ar kiberdrošību.
- **2. līmenis: procesu izstrāde**
  Šā līmeņa mērķis ir palīdzēt pašvaldībām izveidot un uzlabot drošības procesus, kas vajadzīgi, lai efektīvi novērstu kiberdrošības problēmas.
- **3. līmenis: informācijas efektīva izmantošana**
  Mērķis ir uzlabot informācijas kopīgošanas mehānismus pašvaldībā, lai pašvaldība varētu efektīvi apzināt sakarības starp šķietami nesaistītām informācijas vienībām.
- **4. līmenis: taktikas izstrāde**
  Šā līmeņa elementi ir paredzēti tam, lai varētu izstrādāt labākas un vairāk proaktīvas metodes uzbrukumu atklāšanai un reaģēšanai uz tiem. Šajā līmenī vairumam prevencijas metožu vajadzētu jau būt ieviestām.
- **5. līmenis: pilnas darbības spējas drošības jomā**
  Šajā līmenī ir iekļauti tie elementi, kam vajadzētu būt ieviestiem ikvienā organizācijā, kas vēlas tikt uzskatīta par darbības ziņā pilnīgi gatavu stāties pretī jebkura veida kiberdraudam.

31. attēls. Kopsavilkums par *CCSMM* virzieniem katrā līmenī

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

Level 1 Security Aware	1. līmenis Drošības apzināšanās
Level 2 Process Development	2. līmenis Procesu izstrāde
Level 3 Information Enabled	3. līmenis Informācijas efektīva izmantošana
Level 4 Tactics Development	4. līmenis Taktikas izstrāde
Level 5 Full Security Operational Capability	5. līmenis Pilnas darbības spējas drošības jomā
Threats Addressed	Novēršamie draudi
Metrics	Rādītāji
Information sharing	Informācijas kopīgošana
Technology	Tehnoloģijas
Training	Apmācība
Test	Testēšana
Unstructured	Nestrukturēti

Governement Industry Citizens	Valdība Nozare Iedzīvotāji
Information Sharing Committee	Informācijas kopīgošanas komiteja
Rosters, GETS, Assess Controls, Encryption	Personu saraksti, *GETS*, piekļuves kontroles, šifrēšana
1-dat Community Seminar	Vienas dienas pašvaldības seminārs
Dark Screen – EOC	*Dark Screen — EOC*
Unstructured	Nestrukturēti
Governement Industry Citizens	Valdība Nozare Iedzīvotāji
Community Security Web site	Pašvaldības drošības tīmekļa vietne
Secure Web Site Firewalls, Backups	Droša tīmekļa vietne, ugunsmūri, dublējumkopijas
Conudcting a CCSE	*CCSE* apmācība
Community Dark Screen	Pašvaldības *Dark Screen*
Structured	Strukturēti
Governement Industry Citizens	Valdība Nozare Iedzīvotāji
Information Correlation Center	Informācijas korelācijas centrs
Event Correlation SW IDS/IPS	Notikumu korelācijas programmatūra, *IDS/IPS*
Vulnerability Assessment	Neaizsargātības novērtējumi
Operational Dark Screen	Darbības *Dark Screen*
Structured	Strukturēti
Governement Industry Citizens	Valdība Nozare Iedzīvotāji
State/Fed Correlation	Štata/valsts korelācija
24/7 manned operations	Nepārtrauktas darbības ar cilvēku līdzdalību
Operational Security	Darbības drošība
Limited Black Demon	Ierobežotas *Black Demon* mācības
Highly Structured	Ļoti strukturēts
Complete Info Vision	Pilnīgāks info redzējums
Automated Operations	Automatizētas darbības
Multi-Discipline Red Teaming	Daudzdisciplīnu sarkanās komandas pārbaude (*red teaming*)
Black Demon	*Black Demon*

Novērtēšanas metode

Ir paredzēts, ka pašvaldības izmanto *CCSMM* kā novērtēšanas metodiku ar ievaddatiem no štata un federālajām tiesībaizsardzības iestādēm. Tā mērķis ir palīdzēt pašvaldībai noteikt, kas ir vissvarīgākais, kuri ir visticamākie uzbrukumu mērķi un kas ir jāaizsargā (un cik spēcīgi). Ņemot vērā šos mērķus, var izstrādāt plānus, lai katra pašvaldības aspekta kiberdrošības gatavības līmeni paaugstinātu līdz vajadzīgajam. *CCSMM* ģenerētā konkrētā informācija palīdz noteikt dažādu tādu testu un mācību mērķus, ko var izmantot, lai novērtētu izveidoto programmu efektivitāti.

A.7 Informācijas drošības gatavības modelis *NIST* kiberdrošības sistēmai (*ISMM*)

Informācijas drošības gatavības modelis (*ISMM*) ir izstrādāts Karaļa Fahda Naftas un minerālu universitātes Datorzinātņu un inženierijas koledžā Saūda Arābijā. Tas ir jauns spēju gatavības modelis, ar ko novērtēt kiberdrošības pasākumu īstenošanu. *ISMM* mērķis ir dot organizācijām iespēju, regulāri izmantojot vienu un to pašu mērīšanas rīku, izmērīt, kā īstenošana ir progresējusi laika gaitā, lai nodrošinātu, ka tiek uzturēts paredzētais drošības stāvoklis. *ISMM* tika izstrādāts 2017. gadā.

Atribūti/virzieni

ISMM ir izmantotas jau pastāvošās *NIST* sistēmas novērtējamās jomas un ir pievienots atbilstības novērtēšanas virziens. Tādējādi modelī organizācijas drošības stāvoklis tiek **novērtēts 23 jomās**. 23 vērtētās jomas ir šādas:

i līdzekļu pārvaldība
ii darbības vide;
iii pārvaldība;
iv riska novērtēšana;
v riska pārvaldības stratēģija;
vi atbilstības novērtēšana;
vii piekļuves kontrole;
viii apzināšanās un apmācība;
ix datu drošība;
x informācijas aizsardzības procesi un procedūras;
xi uzturēšana;
xii aizsardzības tehnoloģijas;
xiii anomālijas un notikumi;
xiv nepārtraukta drošības uzraudzība;
xv atklāšanas procesi;
xvi reaģēšanas plānošana;
xvii reaģēšanas sakari;
xviii reaģēšanas analīze;
xix reaģēšana seku mazināšanai;
xx reaģēšanas uzlabojumi;
xxi atkopšanas plānošana;
xxii atkopšanas uzlabojumi;
xxiii atkopšanas sakari.

Gatavības līmeņi

ISMM ir **pieci gatavības līmeņi**, kuri pieejamajā dokumentācijā diemžēl nav aplūkoti sīkāk:

- **1. līmenis:** izpildīts process;
- **2. līmenis:** pārvaldīts process;
- **3. līmenis:** labi nostiprināts process;
- **4. līmenis:** paredzams process;
- **5. līmenis:** process, kas uzlabojas.

Novērtēšanas metode

ISMM nav piedāvāta konkrēta metodika, saskaņā ar kuru varētu novērtēt organizācijas.

A.8 Iekšējās revīzijas spēju modelis (*IA-CM*) publiskajam sektoram

Iekšējās revīzijas spēju modeli (*IA-CM*) izstrādāja Iekšējo revidentu institūta Pētniecības fonds, lai ar pašnovērtējumu vairotu spējas un atbalstu publiskajā sektorā. *IA-CM* ir paredzēts revīzijas speciālistiem un sniedz pārskatu par pašu modeli, kā arī lietošanas norādījumus par to, kā modeli izmantot par pašnovērtēšanas rīku.

Lai arī *IA-CM* ir vērsts uz iekšējās revīzijas spējām, nevis kiberdrošības spēju veidošanu, tas ir veidots kā gatavības pašnovērtēšanas rīks publiskā sektora struktūrām un to var izmantot vispārēji procesu un efektivitātes uzlabošanai. Tā kā modeļa darbības joma nav vērsta uz kiberdrošību, tā atribūti netiks analizēti. *IA-CM* tika pabeigts 2009. gadā.

Gatavības līmeņi

Iekšējās revīzijas spēju modelim (*IA-CM*) ir **pieci gatavības līmeņi**, un katrā no tiem ir aprakstītas līmenim raksturīgās iekšējās revīzijas darbību īpašības un spējas. Modeļa spēju līmeņi ir ceļvedis pastāvīgai rezultātu uzlabošanai.

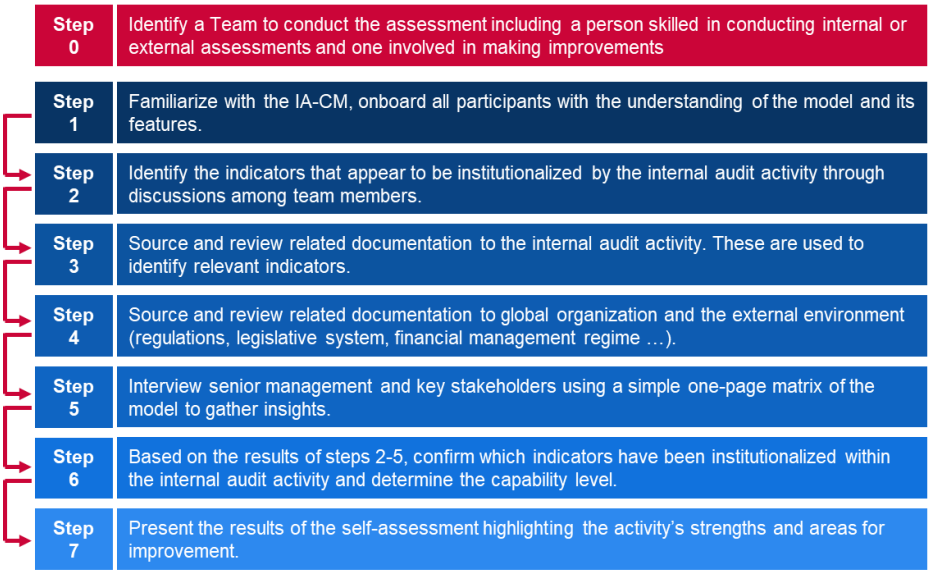
- **1. līmenis: sākotnējais**
  Nav ilgtspējīgu, atkārtojamu spēju, tās ir atkarīgas no individuāliem centieniem.
  - *Ad hoc* vai nestrukturētas.
  - Izolēti, atsevišķi dokumentu un darījumu revīzijas vai pārskatīšanas gadījumi, kuru mērķis ir novērtēt to pareizību un atbilstību.
  - Iznākums ir atkarīgs no tā, cik prasmīga ir persona, kas ieņem attiecīgo amatu.
  - Ir ieviestas tikai tādas profesionālās prakses, ko noteikušas profesionālās asociācijas.
  - Finansējumu apstiprina vadība pēc vajadzības.
  - Infrastruktūras nav.
  - Revidenti visbiežāk ir daļa no lielākas organizatoriskās vienības.
  - Institucionālās spējas nav attīstītas.
- **2. līmenis: infrastruktūra**
  Ilgtspējīgas un atkārtojamas prakses un procedūras.
  - Galvenais jautājums vai izaicinājums 2. līmenī ir, kā panākt un saglabāt procesu atkārtojamību un tātad arī atkārtojamas spējas.
  - Tiek veidotas pakļautības struktūras iekšējās revīzijas jomā, vadības un administratīvā infrastruktūra un profesionālās prakses un procesi (iekšējās revīzijas norādījumi, procesi un procedūras).
  - Revīzija principā tiek plānota saskaņā ar vadības prioritātēm.
  - Pastāvīgi paļaujas pamatā uz konkrētu personu prasmēm un kompetenci.
  - Daļēja atbilstība standartiem.
- **3. līmenis: integrēts**
  Vadības un profesionālās prakses tiek piemērotas viendabīgi.
  - Iekšējās revīzijas politika, procesi un procedūras ir noteikti, dokumentēti un integrēti cits citā un organizācijas infrastruktūrā.
  - Iekšējās revīzijas pārvaldības un profesionālās prakses ir labi nostiprinājušās un tiek viendabīgi piemērotas visās iekšējās revīzijas darbībās.
  - Iekšējo revīziju sāk pielāgot organizācijas darbībai un riskiem, ar ko tā saskaras.
  - Iekšējais revidents no personas, kas veic tikai tradicionālu iekšējo revīziju, pārtop par patiesu komandas biedru, kas sniedz padomus par darbības rezultātiem un risku pārvaldību.
  - Galvenā uzmanība ir vērsta uz komandas veidošanu un iekšējās revīzijas darbību spējām, tās neatkarību un objektivitāti.
  - Lielākoties atbilst standartiem.
- **4. līmenis: pārvaldīts**
  Integrē informāciju, kas gūta no visas organizācijas, lai uzlabotu organizācijas un risku pārvaldību.
  - Iekšējā revīzija saskan ar galveno ieinteresēto personu gaidām.
  - Ir ieviesti darbības rādītāji, ar ko mērīt un uzraudzīt iekšējās revīzijas procesus un rezultātus.
  - Tiek atzīts, ka iekšējā revīzija sniedz būtisku ieguldījumu organizācijā.
  - Iekšējā revīzija ir neatņemama organizācijas pārvaldības un riska pārvaldības daļa.
  - Iekšējā revīzija ir labi pārvaldīta organizācijas struktūrvienība.
  - Riskus mēra un pārvalda kvantitatīvi.
  - Ir ieviestas vajadzīgās prasmes un kompetence, un ir iespējas tās atjaunot un dalīties zināšanās (gan iekšējās revīzijas dalībnieku starpā, gan visas organizācijas mērogā).
- **5. līmenis: uzlabojošies**
  Mācīšanās gan no organizācijas, gan no ārējiem dalībniekiem, lai nepārtraukti uzlabotos.
  - Iekšējā revīzija ir struktūrvienība, kas nepārtraukti mācās, uzlabo procesus un ievieš jauninājumus.
  - Iekšējā revīzija izmanto informāciju gan no organizācijas, gan ārējiem dalībniekiem, lai palīdzētu sasniegt stratēģiskos mērķus.
  - Darbība atbilst pasaules līmenim / ieteikumiem / paraugpraksei.
  - Iekšējā revīzija ir kritiski svarīga organizācijas pārvaldības struktūras daļa.
  - Augstākā līmeņa profesionālas un speciālas prasmes.
  - Individuālā, struktūrvienības un organizācijas snieguma rādītāji ir pilnīgi integrēti, lai

- veicinātu darbības rezultātu uzlabošanos.

Novērtēšanas metode

Iekšējās revīzijas spēju modelis ir acīmredzami veidots pašnovērtējuma veikšanai. Tajā ir sniegti detalizēti norādījumi, kā izmantot *IA-CM*, un pielāgojamu slaidu paraugu komplekts. Pirms pašnovērtēšanas sākuma ir jāieceļ īpaša grupa, kurā ir vismaz viena persona, kam ir labas prasmes iekšējās revīzijas iekšējo vai ārējo novērtējumu veikšanā, un viena persona, kas ir iesaistīta uzlabojumu veikšanā šajā jomā.

12. attēls. *IA-CM* pašnovērtēšanas soļi



Step 0	0. solis
Step 1	1. solis
Step 2	2. solis
Step 3	3. solis
Step 4	4. solis
Step 5	5. solis
Step 6	6. solis
Step 7	7. solis
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Ieceliet novērtēšanas grupu, kurā ir persona ar labām prasmēm iekšējo vai ārējo novērtējumu veikšanā un persona, kas iesaistīta uzlabojumu veikšanā.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Iepazīstieties ar *IA-CM*, informējiet visus dalībniekus, kā ir jāsaprot modelis un tā elementi.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Grupas dalībnieku diskusijās nosakiet rādītājus, kuri iekšējās revīzijas darbību rezultātā, šķiet, ir institucionalizēti.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Iegūstiet un pārskatiet ar iekšējās revīzijas darbībām saistīto dokumentāciju. To izmanto, lai noteiktu attiecīgus rādītājus.
Source and review realted documentation to global organisation and the external	Iegūstiet un pārskatiet dokumentāciju, kas saistīta ar organizāciju kopumā un ar ārējo vidi

environment (regulations, legislative system, financial management regime …).	(noteikumus, tiesību aktu sistēmu, finanšu pārvaldības režīmu utt.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Intervējiet augstākā līmeņa vadītājus un galvenās ieinteresētās personas, izmantojot vienkāršu, vienu lappusi garu modeļa matricu, lai apkopotu viedokļus.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Pamatojoties uz 2.–5. soļa rezultātiem, apstipriniet, kuri rādītāji ir institucionalizēti iekšējās revīzijas darbībās, un nosakiet spēju līmeni.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Iepazīstiniet ar pašnovērtējuma rezultātiem, izceļot darbību stiprās puses un jomas, kuras būtu jāuzlabo.

A.9 Globālais kiberdrošības indekss (*GCI*)

Globālais kiberdrošības indekss (*GCI*) ir Starptautiskās Telesakaru savienības (*ITU*) iniciatīva, kuras mērķis ir pārskatīt apņēmīgumu un situāciju kiberdrošības jomā visos *ITU* reģionos — Āfrikā, Amerikā, arābu valstīs, Āzijas un Klusā okeāna reģionā, NVS un Eiropā — un kura izceļ valstis ar spēcīgu apņemšanos un ieteicamām praksēm. *GCI* nolūks ir palīdzēt valstīm noteikt sfēras, kurās nepieciešami uzlabojumi kiberdrošības jomā, kā arī motivēt tās rīkoties, lai uzlabotu savu vietu novērtējuma tabulā, tādējādi palīdzot paaugstināt kiberdrošības kopējo līmeni pasaulē.

Tā kā *GCI* ir indekss, nevis gatavības modelis, tajā valstu un reģionu vispārējais apņēmīgums kiberdrošības īstenošanā tiek novērtēts un salīdzināts, izmantojot vērtējumu punktos, nevis gatavības līmeņus.

Atribūti/virzieni

Globālais kiberdrošības indekss (*GCI*) ir balstīts uz pieciem Globālās kiberdrošības programmas (*GCA*) pīlāriem. Šie pīlāri veido piecus *GCI* apakšindeksus, un katrs no tiem iekļauj vairākus rādītājus. Pieci pīlāri un rādītāji ir šādi:

i **tiesiskais**: mērījumi, kuri ir atkarīgi no tā, vai pastāv tiesiskās iestādes un regulējums, kas attiecas uz kiberdrošību un kibernoziedzību:
- tiesību akti par kibernoziedzību;
- noteikumi par kiberdrošību;
- tiesību akti par surogātpasta ierobežošanu/samazināšanu;

ii **tehniskais**: mērījumi, kas ir atkarīgi no tā, vai pastāv tehniskas iestādes un satvari, kuri attiecas uz kiberdrošību:
- *CERT/CIRT/CSRIT*;
- standartu īstenošanas satvars;
- standartizācijas iestāde;
- tehniskie mehānismi un spējas, ko izmanto, lai vērstos pret surogātpastu;
- mākoņa izmantošana kiberdrošības vajadzībām;
- mehānismi bērnu aizsardzībai tiešsaistē;

iii **organizatoriskais**: mērījumi, kas atkarīgi no tā, vai pastāv politikas koordinācijas iestādes un stratēģijas kiberdrošības attīstībai valsts līmenī:
- valsts kiberdrošības stratēģija;
- atbildīgā aģentūra;
- kiberdrošība;

iv **spēju veidošana**: mērījumi, kas atkarīgi no tā, vai pastāv pētniecības un izstrādes, izglītības un apmācības programmas, sertificēti profesionāļi un publiskā sektora aģentūras, kas veicina spēju veidošanu:
- sabiedrības izpratnes vairošanas kampaņas;
- kiberdrošības profesionāļu sertifikācijas un akreditācijas sistēma;
- profesionāļu apmācības kursi kiberdrošības jomā;

- izglītības programmas vai akadēmiskas mācību programmas kiberdrošības jomā;
- kiberdrošības pētniecības un izstrādes programmas;
- stimulu mehānismi;

v **sadarbība**: mērījumi, kas atkarīgi no tā, vai pastāv partnerības, sadarbības sistēmas un informācijas kopīgošanas tīkli:

- divpusēji nolīgumi;
- daudzpusēji nolīgumi;
- dalība starptautiskos forumos/asociācijās;
- publiskā un privātā sektora partnerība;
- aģentūru savstarpējā / aģentūras iekšējā partnerība;
- paraugprakse.

Novērtēšanas metode

GCI ir pašnovērtēšanas rīks, kas veidots, izmantojot anketu[30] ar bināriem jautājumiem, kuriem ir iepriekš noteikti atbilžu varianti, un atvērtiem jautājumiem. Izmantojot bināras atbildes, tiek novērsts subjektīvs vērtējums un iespējama tendence izvēlēties kāda konkrēta veida atbildes. Iepriekš noteiktie atbilžu varianti ietaupa laiku un ļauj precīzāk analizēt datus. Turklāt vienkārša dihotoma skala ļauj veikt ātrāku un kompleksāku izvērtējumu, jo nav vajadzīgas garas atbildes, tāpēc atbilžu sniegšana un pēc tam arī to izvērtēšana tiek paātrināta un racionalizēta. Respondentam tikai jāapstiprina konkrētu iepriekš noteiktu kiberdrošības risinājumu esība vai neesība. Tiešsaistes aptaujas mehānisms, ko izmanto atbilžu apkopošanai un attiecīgu materiālu augšupielādei, dod iespēju ekspertu grupai izgūt labu praksi un veikt vairākus tematiskus kvalitatīvos izvērtējumus.

Viss *GCI* process noris šādi.

- Visiem dalībniekiem nosūta uzaicinājuma vēstuli, kurā viņus informē par iniciatīvu un lūdz norādīt kontaktpunktu, kas būs atbildīgs par visu attiecīgo datu vākšanu un *GCI* tiešsaistes anketas aizpildīšanu. Tiešsaistes aptaujas laikā *ITU* oficiāli aicina apstiprināto kontaktpunktu aizpildīt anketu.
- Primāro datu vākšana (par valstīm, kas neaizpilda anketu):
  - *ITU* izstrādā atbilžu uz anketas jautājumiem sākotnēju projektu, izmantojot publiski pieejamus datus un internetā pieejamu informāciju;
  - anketas atbilžu projektu nosūta kontaktpunktiem pārskatīšanai;
  - kontaktpunkti precizē anketas atbilžu projektu un tad to nosūta atpakaļ;
  - izlaboto anketas atbilžu projektu nosūta katram kontaktpunktam galīgajai apstiprināšanai;
  - apstiprinātās anketas atbildes izmanto analīzei, vērtējuma piešķiršanai un ierindošanai vērtējumu tabulā.
- Sekundāro datu vākšana (par valstīm, kas aizpilda anketu):
  - *ITU* nosaka, kuru atbilžu, apliecinošu dokumentu, saišu utt. trūkst;
  - kontaktpunkts vajadzības gadījumā precizē atbildes;
  - izlaboto anketas atbilžu projektu nosūta katram kontaktpunktam galīgajai apstiprināšanai;
  - apstiprinātās anketas atbildes izmanto analīzei, vērtējuma piešķiršanai un ierindošanai vērtējumu tabulā.

A.10 Kiberspēcīguma indekss (*CPI*)

[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

Kiberspēcīguma indeksu (*CPI*) 2011. gadā izveidoja uzņēmuma "Booz Allen Hamilton" sponsorētā organizācijas "The Economist Intelligence Unit" pētniecības programma. *CPI* ir "dinamisks kvantitatīvs un kvalitatīvs modelis, (..) kas mēra konkrētus kibervides atribūtus sadalījumā pa četriem šādiem kiberspēcīguma virzītājspēkiem: tiesiskais un normatīvais regulējums; ekonomiskais un sociālais konteksts; tehnoloģiju infrastruktūra; lietojums nozarēs, kurā tiek aplūkots progress digitālajā jomā galvenajās nozarēs"[31]. Kiberspēcīguma indeksa mērķis ir veikt salīdzinošo vērtējumu G20 valstu spējām izturēt kiberuzbrukumus un ieviest digitālo infrastruktūru, kas nepieciešama plaukstošai un drošai ekonomikai. *CPI* salīdzinošajā vērtējumā tiek aplūkotas 19 G20 valstis (neskaitot ES). Tad indeksā visas valstis tiek sarindotas pēc to vērtējuma katrā rādītājā.

Atribūti/virzieni

Kiberspēcīguma indekss (*CPI*) ir balstīts uz četriem kiberspēju virzītājspēkiem. Katra kategorija tiek novērtēta ar vairākiem rādītājiem, kā rezultātā katrai valstij tiek piešķirts konkrēts vērtējums punktos. Kategorijas un pīlāri ir šādi:

i **tiesiskais un normatīvais regulējums:**
- valdības apņemšanās attīstīt kiberdrošību;
- kiberaizsardzības politika;
- interneta cenzūra (vai tās trūkums);
- politikas efektivitāte;
- intelektuālā īpašuma aizsardzība;

ii **ekonomiskais un sociālais konteksts:**
- izglītības līmenis;
- tehniskās prasmes;
- tirdzniecības atvērtība;
- novatoriskuma pakāpe uzņēmējdarbības vidē;

iii **tehnoloģiju infrastruktūra:**
- piekļuve informācijas un komunikācijas tehnoloģijām;
- informācijas un komunikācijas tehnoloģiju kvalitāte;
- informācijas un komunikācijas tehnoloģiju pieejamība cenas ziņā;
- tēriņi informācijas tehnoloģiju jomā;
- drošu serveru skaits;

iv **lietojums nozarēs:**
- viedie energotīkli;
- e-veselība;
- e-komercija;
- intelektisks transports;
- e-pārvalde.

Novērtēšanas metode

CPI ir kvantitatīvas un kvalitatīvas novērtēšanas modelis. Novērtējumu veica organizācija "The Economist Intelligence Unit", izmantojot pieejamos statistikas avotos balstītus kvantitatīvus rādītājus un aplēses, ja datu nebija. Galvenie izmantotie avoti ir "The Economist Intelligence Unit", ANO Izglītības, zinātnes un kultūras organizācija (*UNESCO*), Starptautiskā Telesakaru savienība (*ITU*) un Pasaules Banka.

A.11 Kiberspēcīguma indekss (*CPI*)

Šajā iedaļā ir rezumēti galvenie konstatējumi, kas izriet no pastāvošo gatavības modeļu analīzes. 5. tabula Pārskats par analizētajiem gatavības modeļiem" pārskats par katra modeļa galvenajām īpašībām saskaņā ar izmainīto Bekera [*Becker*] modeli. 6. tabulā "Gatavības līmeņu salīdzinājums" vispārīgās analizēto modeļu gatavības līmeņu definīcijas. 7. tabulā ir sniegts pārskats par katrā modelī izmantotajiem virzieniem vai atribūtiem.

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

5. tabula. Pārskats par analizētajiem gatavības modeļiem

Modeļa nosaukums	Avotinstitūcija	Mērķis	Mērķauditorija	Līmeņu skaits	Atribūtu skaits	Novērtēšanas metode	Rezultātu atspoguļojums
Kiberdrošības spēju gatavības modelis valstīm (*CMM*)	Globālais kiberdrošības spēju centrs, Oksfordas Universitāte	Vairot kiberdrošības spēju veidošanas apmēru un efektivitāti starptautiskā mērogā	Valstis	5	5 galvenie virzieni	Sadarbība ar vietējo organizāciju, lai precizētu modeli pirms tā piemērošanas valsts kontekstā	Radardiagramma ar 5 sektoriem
Kiberdrošības spēju gatavības modelis (*C2M2*)	ASV Enerģētikas departaments	Palīdzēt organizācijām izvērtēt savas kiberdrošības programmas un tās uzlabot, un stiprināt savu darbības noturību	Visu nozaru, veidu un lielumu organizācijas	4	10 galvenās jomas	Pašizvērtēšanas metodika un rīkkopa	Rādītāju sistēma ar sektoru diagrammām
Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēma	Nacionālais Standartu un tehnoloģijas institūts (*NIST*)	Sistēma, kuras mērķis ir virzīt kiberdrošības darbības un pārvaldīt riskus organizācijās	Organizācijas	n. p. (4 līmeņi)	5 pamatfunkcijas	Pašnovērtējums	-
Kataras kiberdrošības spēju gatavības modelis (*Q-C2M2*)	Kataras Universitātes Tieslietu koledža	Nodrošināt praktiski izmantojamu modeli, ko var lietot, lai salīdzinoši izvērtētu, mērītu un pilnveidotu Kataras kiberdrošības satvaru	Kataras organizācijas	5	5 galvenās jomas	-	-
Kiberdrošības gatavības modeļa sertifikācija (*CMMC*)	ASV Aizsardzības departaments	Veicināt kiberdrošības paraugpraksi, lai aizsargātu informāciju	Aizsardzības rūpnieciskā pamata sektora organizācijas	5	17 galvenās jomas	Ārēju revidentu veikts novērtējums	-
Pašvaldību kiberdrošības gatavības modelis (*CCSMM*)	Teksasas Universitātes Infrastruktūras aizsardzības un drošības centrs	Konstatēt, cik lielā mērā pašvaldība pašlaik ir sagatavota kiberdrošības jomā, un nodrošināt ceļvedi, ko pašvaldības var izmantot par atsauci savos sagatavošanās centienos	Pašvaldības (vietējās vai štata pašvaldības)	5	6 galvenie virzieni	Pašvaldības veikts novērtējums, kurā ieguldījumu sniedz štata un federālās tiesībaizsardzības iestādes	-
Informācijas drošības gatavības modelis *NIST* kiberdrošības satvaram (*ISMM*)	Datorzinātņu un inženierijas koledža, Karaļa Fahda Naftas un minerālu universitāte, *Dhahran*, Saūda Arābija	Dot organizācijām iespēju izmērīt, kā īstenošana ir progresējusi laika gaitā, lai nodrošinātu, ka tās uztur paredzēto drošības stāvokli	Organizācijas	5	23 vērtētas jomas	-	-
Iekšējās revīzijas spēju modelis (*IA-CM*) publiskajam sektoram	Iekšējo revidentu institūta Pētniecības fonds	Ar pašnovērtējumu vairot iekšējās revīzijas spējas un atbalstu publiskajā sektorā	Publiskā sektora organizācijas	5	6 elementi	Pašnovērtējums	-
Globālais kiberdrošības indekss (*GCI*)	Starptautiskā Telesakaru savienība (*ITU*)	Pārskatīt apņēmīgumu un situāciju kiberdrošības jomā un palīdzēt valstīm noteikt sfēras, kurās nepieciešami uzlabojumi kiberdrošības jomā	Valstis	n. p.	5 pīlāri	Pašnovērtējums	Rangu tabula
Kiberspēcīguma indekss (CPI)	Organizācija "The Economist Intelligence Unit" un uzņēmums "Booz Allen Hamilton"	Veikt salīdzinošo vērtējumu G20 valstu spējām izturēt kiberuzbrukumus un ieviest digitālo infrastruktūru, kas nepieciešama plaukstošai un drošai ekonomikai	G20 valstis	n. p.	4 kategorijas	"Economist Intelligence Unit" veikta salīdzinošā vērtēšana	Rangu tabula

6. tabula. Gatavības līmeņu salīdzinājums

Modelis	1. līmenis	2. līmenis	3. līmenis	4. līmenis	5. līmenis
Kiberdrošības spēju gatavības modelis valstīm (CMM)	**Sākumposms** Vai nu nav nekādu kiberdrošības spēju, vai arī tās ir pašā iedīglī. Var būt aizsākušās sākotnējas diskusijas par kiberdrošības spēju veidošanu, bet nekādas konkrētas darbības vēl nav veiktas. Šajā posmā nav novērojami nekādi pierādījumi.	**Veidošanās posms** Dažas aspektu daļas ir sākušas augt un veidoties, taču tām, iespējams, pievēršas tikai pēc vajadzības, tās var būt dezorganizētas, slikti noteiktas vai vienkārši "jaunas". Taču ir skaidri redzami pierādījumi par šādām darbībām.	**Nostiprināšanās posms** Aspekta elementi ir ieviesti un darbojas. Tomēr nav labi pārdomāta attiecīga resursu piešķīruma. Ir pieņemts maz kompromisa lēmumu par "relatīvajiem" ieguldījumiem dažādajos aspekta elementos. Tomēr aspekts ir funkcionāls un noteikts.	**Stratēģiskais posms** Ir izdarītas izvēles attiecībā uz to, kuras aspekta daļas konkrētajai organizācijai vai valstij ir svarīgas un kuras ir mazāk svarīgas. Stratēģiskais posms atspoguļo to, ka šīs izvēles ir izdarītas saskaņā ar valsts vai organizācijas apstākļiem.	**Dinamiskais posms** Ir ieviesti skaidri mehānismi stratēģijas mainīšanai atkarībā no valdošajiem apstākļiem, piem., apdraudējumu vides tehnoloģijām, konfliktiem pasaulē vai būtiskām pārmaiņām kādā problēmjomā (piem., kibernoziedzības vai privātuma jomā). Dinamiskām organizācijām ir labi izstrādātas metodes plūdenai izmaiņu ieviešanai stratēģijās. Šim posmam raksturīga ātra lēmumu pieņemšana, resursu pārdalīšana un nepārtrauktas uzmanības pievēršana mainīgajai videi.
Kiberdrošības spēju gatavības modelis (C2M2)	**0. GRL** Nekāda prakse netiek īstenota.	**1. GRL** Tiek īstenota sākotnēja prakse, bet, iespējams, tikai pēc vajadzības.	**2. GRL** Pārvaldības raksturojums: prakse tiek dokumentēta; procesa atbalstam ir nodrošināti pietiekami resursi; personālam, kas īsteno praksi, ir atbilstošas prasmes un zināšanas; atbildība par prakses īstenošanu un ar prakses īstenošanu saistītās pilnvaras ir piešķirtas konkrētam dalībniekam. Pieejas raksturojums: prakse ir pilnīgāka vai augstāk attīstīta nekā 1. GRL.	**3. GRL** Pārvaldības raksturojums: darbības tiek īstenotas saskaņā ar politiku (vai citiem organizācijas norādījumiem); ir noteikti un tiek uzraudzīti jomas darbību rezultātu mērķi, lai sekotu līdzi sasniegumiem; visā uzņēmumā tiek izmantotas standartizētas, dokumentētas prakses, kas attiecas uz jomas darbībām, un tās tiek uzlabotas. Pieejas raksturojums: prakse ir pilnīgāka vai augstāk attīstīta nekā 2. GRL.	-
Informācijas drošības gatavības modelis NIST kiberdrošības sistēmai (ISMM)	**Izpildīts process**	**Pārvaldīts process**	**Labi nostiprināts process**	**Paredzams process**	**Process, kas uzlabojas**
Kataras kiberdrošības spēju gatavības modelis (Q-C2M2)	**Sākuma** Izmanto *ad hoc* kiberdrošības prakses un procesu dažās jomās.	**Attīstības** Tiek īstenota politika un prakse jomās noteikto kiberdrošības darbību attīstīšanai un uzlabošanai ar mērķi ieteikt jaunas īstenojamas darbības.	**Ieviešanas** Ir pieņemta politika, kurā paredzēts līdz noteiktam laikam īstenot visas jomās noteiktās kiberdrošības darbības.	**Adaptīvais** Tiek atkārtoti aplūkotas un pārskatītas kiberdrošības darbības un pieņemta prakse, pamatojoties uz prognostiskajiem rādītājiem, kas izriet no	**Ātrdarbības** Tiek turpināts adaptīvajā posmā aprakstītais, bet lielāks uzsvars tiek likts uz ātru reakciju un ātrumu darbību īstenošanā jomās.

				iepriekšējās pieredzes un pasākumiem.	
Kiberdrošības gatavības modeļa sertifikācija (CMMC)	**Procesi — tiek īstenoti** Organizācija, iespējams, spēj īstenot šīs prakses tikai tad, kad nepieciešams, un tās var būt vai nebūt dokumentētas. Procesu gatavība 1. līmenī netiek novērtēta. **Prakses — pamata kiberhigiēna** 1. līmenī galvenā uzmanība tiek pievērsta *FLI* (federālo līgumu informācijas) aizsardzībai, un tas ietver tikai tādas prakses, kas atbilst pamata aizsardzības nodrošināšanas prasībām.	**Procesi — ir dokumentēti** 2. līmenī organizācijai jābūt izveidotām un dokumentētām praksēm un politikai, kas virza tās *CMMC* centienu īstenošanu. Ja prakses ir dokumentētas, personas tās var īstenot atkārtoti. Organizācijas uzlabo savas spējas līdz gatavībai, dokumentējot savus procesus un tad tos īstenojot tā, kā norādīts dokumentos. **Prakses — viduvēja kiberhigiēna** 2. līmenis ir pārejas posms no 1. līmeņa uz 3. līmeni un ietver daļu no NIST SP 800-171 noteiktajām drošības prasībām, kā arī prakses no citiem standartiem un atsauces dokumentiem.	**Procesi — tiek pārvaldīti** 3. līmenī organizācijai jāizveido, jāuztur un jāapgādā ar resursiem plāns, kas parāda, kā tiek pārvaldītas prakses īstenošanai nepieciešamās darbības. Plānā var būt iekļauta informācija par uzdevumiem, mērķiem, projektu plāniem, resursiem, nepieciešamo apmācību un attiecīgu ieinteresēto personu iesaisti. **Prakses — laba kiberhigiēna** 3. līmenī uzmanība tiek pievērsta KNI (kontrolētas neklasificētas informācijas) aizsardzībai, un tajā ir ietvertas visas NIST SP 800-171 noteiktās drošības prasības, kā arī papildu prakses no citiem standartiem un atsauces dokumentiem, lai mazinātu apdraudējumu ietekmi.	**Procesi — tiek pārskatīti** 4. līmenī organizācijai jāpārskata prakses un jāvērtē to efektivitāte. Organizācijas šajā līmenī ne tikai vērtē prakšu efektivitāti, bet arī var nepieciešamības gadījumā veikt korektīvas darbības un regulāri informēt augstākā līmeņa vadību par stāvokli vai problēmām. **Prakses — proaktīvas** 4. līmenī galvenā uzmanība tiek pievērsta KNI aizsardzībai, un tajā ir ietverta daļa no pastiprinātajām drošības prasībām. Šīs prakses uzlabo organizācijas atklāšanas un reaģēšanas spējas, lai tā varētu labāk tikt galā ar mainīgajām taktikām, paņēmieniem un procedūrām un pielāgoties tām.	**Procesi — tiek optimizēti** 5. līmenī organizācijai ir jāstandartizē un jāoptimizē procesu īstenošana visā organizācijā. **Prakses — augsti attīstītas / proaktīvas** 5. līmenī galvenā uzmanība tiek pievērsta KNI aizsardzībai. Papildu prakses padziļina un izkopj kiberdrošības spējas.
Pašvaldību kiberdrošības gatavības modelis (CCSMM)	**Drošības apzināšanās** Šā līmeņa pasākumu galvenais mērķis ir likt personām un organizācijām apzināties draudus, problēmas un problēmjautājumus, kas saistīti ar kiberdrošība.	**Procesu izstrāde** Šā līmeņa mērķis ir palīdzēt pašvaldībām izveidot un uzlabot drošības procesus, kas vajadzīgi, lai efektīvi novērstu kiberdrošības problēmas.	**Informācijas efektīva izmantošana** Mērķis ir uzlabot informācijas kopīgošanas mehānismus pašvaldībā, lai pašvaldība varētu efektīvi apzināt sakarības starp šķietami nesaistītām informācijas vienībām.	**Taktikas izstrāde** Šā līmeņa elementi ir paredzēti tam, lai varētu izstrādāt labākas un vairāk proaktīvas metodes uzbrukumu atklāšanai un reaģēšanai uz tiem. Šajā līmenī vairumam prevencijas metožu vajadzētu jau būt ieviestām.	**Pilnas darbības spējas drošības jomā** Šajā līmenī ir iekļauti tie elementi, kam vajadzētu būt ieviestiem ikvienā organizācijā, kas vēlas tikt uzskatīta par darbības ziņā pilnīgi gatavu stāties pretī jebkura veida kiberdraudam.
Iekšējās revīzijas spēju modelis (IA-CM) publiskajam sektoram	**Sākotnējais** Nav ilgtspējīgu, atkārtojamu spēju, tās ir atkarīgas no individuāliem centieniem.	**Infrastruktūra** Ilgtspējīgas un atkārtojamas prakses un procedūras.	**Integrēts** Vadības un profesionālās prakses tiek piemērotas viendabīgi.	**Pārvaldīts** Integrē informāciju, kas gūta no visas organizācijas, lai uzlabotu organizācijas un risku pārvaldību.	**Uzlabojošies** Mācīšanās gan no organizācijas, gan no ārējiem dalībniekiem, lai nepārtraukti uzlabotos.

7. tabula. Atribūtu/virzienu salīdzinājums

	Kiberdrošības spēju gatavības modelis valstīm (CMM)	Kiberdrošības spēju gatavības modelis (C2M2)	Kataras kiberdrošības spēju gatavības modelis (Q-C2M2)	Kiberdrošības gatavības modeļa sertifikācija (CMMC)	Kiberdrošības gatavības modeļa sertifikācija (CMMC)	Informācijas drošības gatavības modelis NIST kiberdrošības sistēmai (ISMM)	Kritiskās infrastruktūras kiberdrošības uzlabošanas sistēma	Globālais kiberdrošības indekss (*GCI*)	Kiberspēcīguma indekss (CPI)
Līmeņi	Pieci virzieni, kas sadalīti vairākos faktoros, kuri, savukārt, iekļauj vairākus aspektus un rādītājus (4. 4.)	10 jomas, kas ietver 1 pārvaldības mērķi un vairākus pieejas mērķus (6. 6.)	Piecas jomas, kas sadalītas apakšjomās	17 jomas, kas iedalītas sīkāk procesos un 1, vairākās vai daudzās spējās, kuras ir sadalītas sīkāk praksēs (9. 9.)	Seši galvenie virzieni	23 vērtētās jomas	Piecas funkcijas ar pamatā esošām galvenajām kategorijām un apakškategorijām (8. 8.).	Pieci pīlāri ar vairākiem rādītājiem	Četras kategorijas ar vairākiem rādītājiem
Atribūti/virzieni	i Kiberdrošības politikas un stratēģijas izstrāde ii Atbildīgas kiberdrošības kultūras veicināšana sabiedrībā iii Kiberdrošības zināšanu pilnveidošana iv Iedarbīga tiesiskā un normatīvā regulējuma izveide v Risku kontrolēšana, izmantojot standartus, organizācijas un tehnoloģijas	i Riska pārvaldība ii Līdzekļu, pārmaiņu un konfigurācijas pārvaldība iii Identitātes un piekļuves pārvaldība iv Apdraudējumu un ievainojamību pārvaldība v Situācijas apzināšanās vi Reaģēšana uz notikumiem un incidentiem vii Piegādes ķēdes un ārējo atkarību pārvaldība viii Darbaspēka pārvaldība ix Kiberdrošības arhitektūra x Kiberdrošības programmas pārvaldība	i Izpratne (kiberpārvaldība, līdzekļi, riski un apmācība) ii Drošība (datu drošība, tehnoloģiju drošība, piekļuves kontroles drošība, sakaru drošība un personāla drošība) iii Riska ietekme (uzraudzība, incidentu pārvaldība, atklāšana, analīze un riska ietekme) iv Reaģēšana (reaģēšanas plānošana, ietekmes mazināšana un saziņa reaģēšanas kontekstā) v Stiprināšana (atkopšanas plānošana, nepārtrauktības pārvaldība, uzlabošana un ārēja atkarība)	i Piekļuves kontrole ii Līdzekļu pārvaldība iii Revīzija un pārskatatbildība iv Apzināšanās un apmācība v Konfigurācijas pārvaldība vi Identificēšana un autentificēšana vii Reaģēšana uz incidentiem viii Uzturēšana ix Informācijas nesēju aizsardzība x Personāla drošība xi Fiziskā aizsardzība xii Atkopšana xiii Riska pārvaldība xiv Drošības novērtēšana xv Situācijas apzināšanās xvi Sistēmu un sakaru aizsardzība xvii Sistēmu un informācijas integritāte	i Novēršamie draudi ii Rādītāji iii Informācijas kopīgošana iv Tehnoloģijas v Apmācība vi Testēšana	i Līdzekļu pārvaldība ii Darbības vide iii Pārvaldība iv Riska novērtēšana v Riska pārvaldības stratēģija vi Atbilstības novērtēšana vii Piekļuves kontrole viii Apzināšanās un apmācība ix Datu drošība x Informācijas aizsardzības procesi un procedūras xi Uzturēšana xii Aizsardzības tehnoloģijas xiii Anomālijas un notikumi xiv Nepārtraukta drošības uzraudzība xv Atklāšanas procesi xvi Reaģēšanas plānošana xvii Reaģēšanas sakari xviii Reaģēšanas analīze xix Reaģēšana seku mazināšanai xx Reaģēšanas uzlabojumi xxi Atkopšanas plānošana xxii Atkopšanas uzlabojumi xxiii Atkopšanas sakari	i Noteikt ii Aizsargāt iii Atklāt iv Reaģēt v Atkopt	i Tiesiskais ii Tehniskais iii Organizatoriskais iv Spēju veidošana v Sadarbība	i Tiesiskais un normatīvais regulējums ii Ekonomiskais un sociālais konteksts iii Tehnoloģiju infrastruktūra iv Lietojums nozarēs

B PIELIKUMS. DOKUMENTU IZPĒTES BIBLIOGRĀFIJA

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

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

Anna, S., u. c., *Stocktaking, analysis and recommendations on the protection of CIIs*, 2016. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML.

Becker, J., Knackstedt, R., u. c., *Developing Maturity Models for IT Management – A Procedure Model and its Application*, 2009. Pieejams vietnē https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Beļģijas valdības kiberdrošības stratēģija, 2012. Pieejama vietnē 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., u. c., *Developing Cybersecurity Capacity: A proof-of-concept implementation guide*, RAND Corporation, 2018. Pieejams vietnē https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf.

Bourgue, R., *Introduction to Return on Security Investment*, 2012.

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

Center for Security Studies (CSS), ETH Zürich, *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*, 2019. Pieejams vietnē 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, "Resolution of the Council of Ministers No. 92/2019", *Portuguese Official Journal*, 1. sērija, Nr. 108, 2019. Pieejams vietnē https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf.

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

CSIRT Maturity - Self-assessment Tool (bez datuma). Pieejams vietnē https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

Eiropas Padomes un Eiropas Savienības projekts *CyberCrime@IPA*, Eiropas Padomes Globālais kibernoziedzības projekts un Eiropas Savienības Kibernoziedzības apkarošanas

darba grupa, *Specialised cybercrime units - Good practice study*, 2011. Pieejams vietnē https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33.

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (bez datuma). Pieejams vietnē https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool.

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

Darra, E., *Welcome to the NCSS Training Tool* (bez datuma).

Dekker, M. A. C., *Technical Guideline on Incident Reporting*, 2014. Pieejams vietnē 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., *Technical Guideline on Security Measures*, 2014. Pieejams vietnē 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., *Guideline on Threats and Assets*, 2015. Pieejams vietnē https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf.

Kiberdrošības stratēģija "Digital Slovenia", 2016. Pieejama vietnē 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., u. c., *Privacy and data protection by design - from policy to engineering*, 2014. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML.

Eiropas Komisija, Eiropas Parlamenta un Padomes regula par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū, 2012. Pieejama vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52012PC0238&from=EN.

Eiropas Tīklu un informācijas drošības aģentūra, *NCSS: Practical Guide on Development and Execution*, Hērakleja: ENISA, 2012.

Eiropas Tīklu un informācijas drošības aģentūra, *NCSS: Setting the course for national efforts to strengthen security in cyberspace*, 2012, Hērakleja: ENISA.

Eiropas Tīklu un informācijas drošības aģentūra, *Guidelines for SMEs on the security of personal data processing*, 2016.

Eiropas Tīklu un informācijas drošības aģentūra, *NCSS good practice guide: designing and implementing national cyber security strategies*, Hērakleja: ENISA, 2016.

Eiropas Savienība un Tīklu un informācijas drošības aģentūra, *Handbook on security of personal data processing*, 2017. Pieejams vietnē http://dx.publications.europa.eu/10.2824/569768.

Eiropas Savienība un Tīklu un informācijas drošības aģentūra, *ENISA CERT inventory inventory of CERT teams and activities in Europe*, 2014. Pieejams vietnē http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe.

Executive Office Of The President, *Memorandum for Heads of Executive Departments and Agencies*, 2015. Pieejams vietnē https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf.

Federal Chancellery of the Republic of Austria, *Austrian Cyber Security Strategy*, 2013. Pieejams vietnē 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, *Cyber Security Strategy for Germany*, 2011. Pieejams vietnē 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., *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*, 2016. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML.

Ferette, L., Eiropas Savienība un Eiropas Tīklu un informācijas drošības aģentūra, *The 2015 report on national and international cyber security exercises: survey, analysis and recommendations*, 2015. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML.

French Prime Minister's Office, *French National Digital Security Strategy*, 2014. Pieejams vietnē https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

Galan Manso, C., u. c., *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, 2015. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML.

Ghent University u. c., "Evaluating Business Process Maturity Models", *Journal of the Association for Information Systems*, 2017. Pieejams vietnē https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais.

Bulgārijas valdība, *National Cyber Security Strategy - Cyber-resistant Bulgaria 2020*, 2015.

Horvātijas valdība, *The National Cyber Security Strategy of The Republic of Croatia*, 2015. Pieejams vietnē https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.

Grieķijas valdība, *National Cyber Security Strategy*, 2017. Pieejams vietnē 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.

Ungārijas valdība, *Strategy for the Security of Network and Information Systems*, 2018. Pieejams vietnē 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.

Īrijas valdība, *National Cyber Security Strategy*, 2019. Pieejams vietnē https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

Spānijas valdība, *National Cyber Security Strategy*, 2019. Pieejams vietnē 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.

Institute of Internal Auditors (red.), *Internal audit capability model (IA-CM) for the public sector: overview and application guide*, Altamontspringsa, Florida: Institute of Internal Auditors, Research Foundation, 2009.

Starptautiskā Telesakaru savienība (ITU), *The Global Cybersecurity Index*, 2018. Pieejams vietnē https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Starptautiskā Telesakaru savienība (ITU), *Guide to developing a national cybersecurity strategy*, 2018. Pieejams vietnē https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

J. D., R. D. B., “Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework”, *International Review of Law*, 2019.

Latvijas valdība, *Cyber Security Strategy of Latvia*, 2014. Pieejams vietnē https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

Liveri, D., u. c., *An evaluation framework for national cyber security strategies*, Hērakleja: ENISA, 2014. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML..

Mattioli, R., u. c., *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks*, 2014. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML.

Ministry for Competitiveness and Digital, Maritime and Services Economy, *Malta Cyber Security Strategy*, 2016. Pieejams vietnē 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, *Cybersecurity Strategy – Republic of Estonia*, 2019. Pieejams vietnē https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Ministry of National Defence Republic of Lithuania, *National Cyber Security Strategy*, 2018.

National Cyber Security Centre, *National Cyber Security Strategy of the Czech Republic*, 2015. Pieejams vietnē https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf.

National Cyber Security Strategies - Interactive Map (bez datuma). Pieejams vietnē https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map..

National Cybersecurity Strategies Evaluation Tool, 2018. Pieejams vietnē https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Gētersberga, Merilenda: National Institute of Standards and Technology, 2018. Pieejams vietnē http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group, *Business Process Maturity Model*, 2008. Pieejams vietnē https://www.omg.org/spec/BPMM/1.0/PDF.

ESAO, Eiropas Savienība un Kopīgais pētniecības centrs — Eiropas Komisija, *Handbook on Constructing Composite Indicators: Methodology and User Guide*, ESAO, 2008. Pieejams vietnē https://www.oecd.org/sdd/42495745.pdf.

Office of the commissioner of Electronic Communications and Postal Regulations, *Cybersecurity Strategy of the Republic of Cyprus*, 2012.

PADOMES DIREKTĪVA 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību, *Eiropas Savienības Oficiālais Vēstnesis*, 2008. Pieejama vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32008L0114&from=EN.

Ekonomiskās sadarbības un attīstības organizācija (ESAO), *Cybersecurity policy making at a turning point*, 2012. Pieejams vietnē http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

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

Ouzounis, E., *Good Practice Guide on National Exercises*, 2012.

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

Presidency of the Council of Ministers, *The Italian Cybersecurity Action Plan*, 2017. Pieejams vietnē 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, *Dziennik Urzędowy Rzeczypospolitej Polskiej*, 2019. Pieejams vietnē http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf.

Rumānijas valdība, *Cyber security strategy of Romania*, 2013. Pieejams vietnē 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., un Eiropas Savienības Kiberdrošības aģentūra, *Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies*, 2019. Pieejams vietnē https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariat of the Security Committee, *Finland's Cyber Security Strategy 2019*, 2019. Pieejams vietnē https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

Slovākijas valdība, *Cyber Security Concept of the Slovak Republic*, 2015. Pieejams vietnē 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., *Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010*, 2015.

Smith, R., "Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010", Smith, R., *Core EU Legislation*, Londona: Macmillan Education, 2016. Pieejams vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V., *European Cyber Security Month 2017*, 2017.

Zviedrijas valdība, *Nationell strategi för samhällets informations- och cybersäkerhet*, 2017. Pieejams vietnē https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view.

The Danish Government - Ministry of Finance, *Danish Cyber and Information Security Strategy*, 2018. Pieejams vietnē https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf.

The Federal Council, *National strategy for the protection of Switzerland against cyber risks*, 2018.

The Luxembourguish Government Council, *National Cybersecurity Strategy*, 2018. Pieejams vietnē 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.

Nīderlandes valdība, *National Cyber Security Agenda*, 2018. Pieejams vietnē 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.

Baltais nams, *National Cyber Strategy of the United States of America*, 2018. Pieejams vietnē https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., u. c., *Cyber Europe Report*, 2011. Pieejams vietnē https://www.enisa.europa.eu/publications/ce2010report.

Trimintzios, P., Gavrila, R., un Eiropas Tīklu un informācijas drošības aģentūra, *National-level risk assessments: an analysis report*, 2013. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML.

Trimintzios, P., Gavrila, R., u. c., *Report on cyber-crisis cooperation and management*, 2015. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML.

Trimintzios, P., Ogee, A., u. c., *Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises*, 2015. Pieejams vietnē http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML.

UK National Cyber Security Strategy 2016-2021, 2016. Pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck u. c., *Understanding Maturity Models*, 2009.

Wamala, D. F., *ITU National Cybersecurity Strategy Guide*, 2011. Pieejams vietnē https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

White, G., “The Community Cyber Security Maturity Model”, *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, 2007.

C PIELIKUMS. CITI APLŪKOTIE MĒRĶI

Tālāk izklāstītie mērķi tika aplūkoti dokumentu izpētes posmā un *ENISA* veiktajās intervijās. Šie mērķi neietilpst valsts spēju novērtēšanas sistēmā, bet izgaismo tematus, ko būtu vērts apspriest. Katrā nākamajā sadaļā ir paskaidrots, kāpēc konkrētais mērķis tika atmests:

- izstrādāt nozaru kiberdrošības stratēģijas;
- apkarot dezinformācijas kampaņas;
- nodrošināt augstās tehnoloģijas (5G, *AI*, kvantisko datošanu u. c.);
- nodrošināt datu suverenitāti;
- stimulēt kiberapdrošināšanas nozares attīstību.

Izstrādāt nozaru kiberdrošības stratēģijas

Pieņemot nozaru stratēģijas, kas attiecas uz iejaukšanās pasākumiem un stimuliem konkrētā nozarē, noteikti tiek pastiprinātas decentralizētās spējas. Tās ir īpaši piemērotas dalībvalstīs, kuru pamatpakalpojumu sniedzējiem jāņem vērā dažādi satvari un noteikumi un kur ir daudz cits no cita atkarīgu elementu kiberdrošības horizontāluma dēļ. Vairākās dalībvalstīs patiešām ir dučiem valsts iestāžu un regulatīvo struktūru, kas pārzina katras nozares specifiku un ir pilnvarotas panākt katrai nozarei specifisku noteikumu izpildi.

Piemēram, Dānija īsteno sešas mērķorientētas stratēģijas, kas attiecas uz vissvarīgāko nozaru kiberdrošības un informācijas drošības pasākumiem, lai panāktu spēcīgākas decentralizētās spējas kiberdrošības un informācijas drošības jomā. Katra “nozares vienība” piedalās cita starpā apdraudējumu novērtēšanā nozares mērogā, uzraudzībā, sagatavošanās mācībās, drošības sistēmu izveidē, zināšanu kopīgošanā un norādījumu sagatavošanā. Nozaru stratēģijas attiecas uz šādām nozarēm:

- enerģētika;
- veselības aprūpe;
- transports;
- telesakari;
- finanses;
- jūrniecība.

Citas dalībvalstis ir paudušas interesi par nozaru kiberdrošības stratēģiju izstrādi, kas dotu iespēju atspoguļot visas normatīvās prasības. Tomēr jāņem vērā, ka šāds mērķis var nebūt piemērots visām dalībvalstīm, ņemot vērā to lielumu, valsts politiku un gatavības pakāpi. Tā kā būtu ļoti grūti nodrošināt, ka sistēmā tiek ņemta vērā visu valstu specifika, *ENISA* izlēma šo mērķi sistēmā neiekļaut.

Apkarot dezinformācijas kampaņas

Dalībvalstis savās valsts kiberdrošības stratēģijās paredz aizsargāt tādus pamatprincipus kā cilvēktiesības, pārredzamība un sabiedrības uzticība. Tas ir ļoti svarīgi, īpaši saistībā ar dezinformāciju, kas tiek izplatīta tradicionālos ziņu medijos vai sociālo plašsaziņas līdzekļu platformās. Turklāt kiberdrošība pašlaik ir viens no lielākajiem problēmjautājumiem saistībā ar vēlēšanām. Dažādās valstīs pirms svarīgām vēlēšanām ir novērotas tādas darbības kā nepatiesas informācijas vai negatīvas propagandas izplatīšana. Šis apdraudējums var pavājināt

ES demokrātisko procesu. Eiropas mērogā Komisija ir sagatavojusi rīcības plānu[32], lai pastiprinātu dezinformācijas apkarošanas centienus Eiropā; šis plāns pievēršas četrām galvenajām jomām (atklāšana, sadarbība savā starpā, sadarbība ar tiešsaistes platformām un informētība), un tā mērķis ir veidot ES spējas un stiprināt sadarbību starp dalībvalstīm.

Četras no 19 intervētajām valstīm ir paudušas nodomu pievērsties dezinformācijas un propagandas problēmai savā VKS.

Piemēram, Francijas VKS[33] ir teikts, ka "valstij ir pienākums informēt iedzīvotājus par manipulācijas riskiem un propagandas paņēmieniem, ko izmanto ļaunprātīgi interneta lietotāji. Piemēram, pēc 2015. gada janvārī Francijā notikušajiem teroristu uzbrukumiem valdība izveidoja informācijas platformu par riskiem, kas saistīti ar islāma radikalizāciju, kurai izmanto elektronisko sakaru tīklus, — "Stop-djihadisme.gouv.fr"". Šo pieeju varētu izmantot, reaģējot arī uz citām propagandas vai destabilizācijas izpausmēm.

Vēl viens piemērs ir Polijas 2019.–2024. gada VKS[34], kurā norādīts, ka "pret manipulatīvām darbībām, piemēram, dezinformācijas kampaņām, ir jāvēršas sistēmiski, lai vairotu iedzīvotāju informētību par informācijas autentiskuma pārbaudīšanu un reaģēšanu uz mēģinājumiem informāciju sagrozīt".

Tomēr *ENISA* veiktajās intervijās vairākas dalībvalstis norādīja, ka tās nevis aplūko šo jautājumu VKS kā kiberdraudu, bet gan cīnās pret to kā pret plašāku sabiedrības problēmu, piemēram, ar politikas iniciatīvām.

Nodrošināt augstās tehnoloģijas (5G, *AI*, kvantisko datošanu u. c.)

Tā kā pašreizējā kiberdraudu aina turpina paplašināties, tad, attīstoties jaunām tehnoloģijām, visticamāk, palielināsies kiberuzbrukumu intensitāte un skaits, kā arī dažādosies apdraudētāju izmantoto metožu, līdzekļu un mērķu klāsts. Tai pašā laikā šie jaunie tehnoloģiskie risinājumi, kas ir augstās tehnoloģijas, var kļūt par Eiropas digitālo tirgu veidojošiem elementiem. Lai pasargātu dalībvalstis no riskiem, ko rada augošā atkarība no digitāliem risinājumiem un jaunu tehnoloģiju rašanās, būtu jāievieš stimuli un pilnvērtīgi izstrādāta politika, kas atbalstītu šo tehnoloģiju drošu un uzticamu izstrādi un izvēršanu ES.

Dalībvalstu VKS dokumentu izpētes posmā tika secināts, ka dalībvalstis interesē šādas augstās tehnoloģijas: 5G, mākslīgais intelekts, kvantiskā datošana, kriptogrāfija, perifērdatošana, satīkloti un autonomi transportlīdzekļi, lielie un viedie dati, blokķēde, robotika un lietu internets.

Konkrētāk, 2020. gada sākumā Eiropas Komisija publicēja paziņojumu, aicinot dalībvalstis rīkoties, lai īstenotu pasākumu kopumu, kas tika ieteikts secinājumos par 5G instrumentu kopumu[35]. Šis 5G instrumentu kopums tika izveidots pēc Komisijas 2019. gadā pieņemtā Ieteikuma (ES) 2019/534 par 5G tīklu kiberdrošību, kurā tika aicināts Eiropā izmantot vienotu pieeju 5G tīklu drošībai[36].

ENISA veiktajās intervijās atklājās, ka šis temats ir vairāk horizontāls un vijas cauri VKS, nevis ir atsevišķi nodalīts mērķis.

[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/LV/TXT/?uri=CELEX%3A32019H0534.

Nodrošināt datu suverenitāti

No vienas puses, kibertelpu var uzskatīt par brīnišķīgu, globālu, kopēju telpu, kurai var viegli piekļūt, kura nodrošina augstu savienojamības pakāpi un kura var sniegt lielas iespējas sociālekonomiskajai izaugsmei. No otras puses, kibertelpai ir vāja jurisdikcija, tajā ir grūti noteikt darbības darītāju, tai nav skaidri noteiktu robežu un ir savstarpēji savienotas sistēmas, kurās var būt pret ielaušanos pietiekami neaizsargātas vietas un kuru datus var nozagt vai kuru datiem pat var piekļūt citu valstu valdības. Līdztekus šiem diviem apsvērumiem jāmin arī tas, ka digitālajā ekosistēmā tiešsaistes pakalpojumu platformas un infrastruktūra bieži vien koncentrējas tikai dažu ieinteresēto personu rokās. Visu iepriekš minēto apsvērumu dēļ dalībvalstis veicina digitālo suverenitāti. Ja ir sasniegta digitālā suverenitāte, iedzīvotāji un uzņēmumi var pilnvērtīgi darboties, izmantojot uzticamus digitālos pakalpojumus un IKT produktus bez bažām par saviem persondatiem, digitālajām vērtībām, ekonomisko neatkarību vai politisko ietekmi.

Datu suverenitātes vai digitālās suverenitātes jomā dalībvalstis ir panākušas lielu progresu gan valsts, gan Eiropas līmenī. Dalībvalstis šo jautājumu parasti neaplūko savās VKS tieši, kā atsevišķu mērķi, taču tās to uzlūko kā horizontālu principu vai arī savu nodomu nodrošināt digitālo suverenitāti valsts līmenī, pievēršoties svarīgākajām tehnoloģijām, pauž *ad hoc* publikācijās. Piemēram, Francijas 2018. gada stratēģiskajā pārskatā par kiberaizsardzību ir norādīts — "lai nodrošinātu digitālo suverenitāti, ir ārkārtīgi svarīgi kontrolēt šādas tehnoloģijas: saziņas šifrēšanu, kiberuzbrukumu atklāšanu, profesionālos mobilos radiosakarus, mākoņdatošanu un mākslīgo intelektu"[37].

Eiropas līmenī dalībvalstis aktīvi piedalās Eiropas Datu stratēģijas (COM(2020) 66 final) formulēšanā un ES Kiberdrošības aktā (Regula (ES) 2019/881) paredzētā IKT digitālo produktu, pakalpojumu un procesu ES sertifikācijas satvara veidošanā, lai nodrošinātu stratēģisku digitālo autonomiju Eiropas līmenī.

Posmā, kurā tika intervētas dalībvalstis, apliecinājās, ka digitālās suverenitātes tēma bieži tiek aplūkota kā plašāks, ne tikai ar kiberdrošību saistīts jautājums. Tāpēc dalībvalstis parasti neiekļauj šo jautājumu savās VKS, bet tās dažas, kas tomēr to ir ietvērušas savā stratēģijā, nav to izdalījušas kā atsevišķu mērķi.

Stimulēt kiberapdrošināšanas nozares attīstību

Pašreizējais stāvoklis kiberapdrošināšanas nozarē liecina, ka globālais tirgus ir neapšaubāmi audzis. Taču tas vēl ir tikai sākumposmā, jo vēl ir jāvāc dati un jānonāk līdz daudziem precedentiem (piem., skaidri neatrunātais segums, sistēmiskie kiberdrošības riski). Turklāt aplēstie kiberuzbrukumu radītie kopējie zaudējumi visā pasaulē ir vairākkārt lielāki nekā pašreizējās kiberapdrošināšanas nozares seguma spēja (SVF darba dokuments "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment", WP/18/143). Taču kiberapdrošināšanas nozares attīstīšana noteikti var dot ieguvumus un likt pamatus pozitīvās mijiedarbības mehānismiem. Kiberapdrošināšanas mehānismi var palīdzēt:

- vairot izpratni par kiberdrošības riskiem uzņēmumos;
- kvantitatīvi izvērtēt pakļautību kiberdrošības riskiem;
- uzlabot kiberdrošības riska pārvaldību;
- sniegt atbalstu organizācijām, kas ir cietušas kiberuzbrukumos;
- atlīdzināt kiberuzbrukuma nodarīto kaitējumu (materiālu vai nemateriālu).

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

Dažas dalībvalstis jau ir sākušas darboties šajā jomā. Piemēram:

- Igaunija savā VKS izmanto nogaidīšanas pieeju: “Lai mazinātu kiberdrošības riskus privātajā sektorā kopumā, tiks analizēts kiberapdrošināšanas pakalpojuma pieprasījums un piedāvājums Igaunijā un, pamatojoties uz analīzes rezultātiem, tiks panākta vienošanās par iesaistīto pušu sadarbības principiem, tostarp informācijas kopīgošanu, riska novērtējuma sagatavošanu utt. Pašlaik Igaunijas tirgū ir maz kiberapdrošināšanas pakalpojumu sniedzēju, un vispirms ir jāapzina, kurš ko piedāvā. Apdrošināšanas piedāvātās aizsardzības sarežģītību bieži vien uzskata par kavēkli kiberapdrošināšanas tirgus attīstībai.”;
- Luksemburga savā VKS ir skaidri paudusi atbalstu kiberapdrošināšanas nozares attīstībai: “1. mērķis: radīt jaunus produktus un pakalpojumus. Lai apvienotu riskus un mudinātu digitālos kiberdrošības incidentos cietušos lūgt palīdzību ekspertiem incidenta pārvarēšanā un ļaunprātīgajā darbībā cietušās sistēmas atjaunošanā, apdrošināšanas sabiedrības tiks mudinātas veidot īpašus produktus kiberapdrošināšanas jomā.”

Intervēto viedokļi šajā jautājumā bija diezgan atšķirīgi — dažas dalībvalstis minēja, ka kiberapdrošināšanas jautājums nesen ir kļuvis par diskusiju tematu, bet citas atzina, ka, lai gan šis virziens ir daudzsološs, nozare vēl nav tam pietiekami gatava. Taču daudz intervēto norādīja, ka šis temats VKS nav aplūkots vai nu tāpēc, ka tas tika uzskatīts par pārāk specifisku, vai arī tāpēc, ka tas neietilpa VKS darbības jomā.

TP-02-21-253-LV-N

Par Eiropas Savienības Kiberdrošības aģentūru

Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir Savienības aģentūra, kuras mērķis ir panākt vienādi augsta līmeņa kiberdrošību visā Eiropā. Eiropas Savienības Kiberdrošības aģentūra, kas dibināta 2004. gadā un nostiprināta ar ES Kiberdrošības aktu, sniedz ieguldījumu ES kiberdrošības politikā, stiprina IKT produktu, pakalpojumu un procesu uzticamību ar kiberdrošības sertifikācijas shēmām, sadarbojas ar dalībvalstīm un ES struktūrām un palīdz Eiropai sagatavoties nākotnes izaicinājumiem kiberdrošības jomā. Daloties zināšanās, veidojot spējas un veicinot izpratni, aģentūra sadarbojas ar savām galvenajām ieinteresētajām personām, lai vairotu uzticību savienotajai ekonomikai, palielinātu Savienības infrastruktūras noturību un visbeidzot garantētu Eiropas sabiedrībai un iedzīvotājiem digitālo drošību. Plašāku informāciju skatiet vietnē 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: 978-92-9204-489-3
DOI: 10.2824/379613