I

(Resolucije, priporočila in mnenja)

PRIPOROČILA

EVROPSKI ODBOR ZA SISTEMSKA TVEGANJA

PRIPOROČILO ODBORA ZA SISTEMSKA TVEGANJA

z dne 2. decembra 2021

o vseevropskem okviru za usklajevanje v primeru sistemskih kibernetskih incidentov za ustrezne organe

(ESRB/2021/17)

(2022/C 134/01)

SPLOŠNI ODBOR EVROPSKEGA ODBORA ZA SISTEMSKA TVEGANJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Sporazuma o Evropskem gospodarskem prostoru ([1]), zlasti Priloge IX k Sporazumu,

ob upoštevanju Uredbe (EU) št. 1092/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o makrobonitetnem nadzoru nad finančnim sistemom Evropske unije in ustanovitvi Evropskega odbora za sistemska tveganja ([2]) ter zlasti člena 3(2)(b) in (d) in členov 16 in 18 Uredbe,

ob upoštevanju Sklepa ESRB/2011/1 Evropskega odbora za sistemska tveganja z dne 20. januarja 2011 o sprejetju Poslovnika Evropskega odbora za sistemska tveganja ([3]) in zlasti členov 18 do 20 Sklepa,

ob upoštevanju naslednjega:

(1) Kakor je navedeno v uvodni izjavi 4 Priporočila ESRB/2013/1 Evropskega odbora za sistemska tveganja ([4]), je končni cilj makrobonitetne politike prispevati k zaščiti stabilnosti celotnega finančnega sistema, vključno s tem, da se okrepi odpornost finančnega sistema in zmanjša kopičenje sistemskih tveganj ter tako zagotovi vzdržen prispevek finančnega sektorja h gospodarski rasti. Evropski odbor za sistemska tveganja (ESRB) je odgovoren za makrobonitetni nadzor finančnega sistema v Uniji. ESRB bi moral pri uresničevanju svojega mandata prispevati k preprečevanju in zmanjševanju sistemskih tveganj za finančno stabilnost, vključno s tistimi, ki so povezana s kibernetskimi incidenti, in predlagati, kako bi ta tveganja lahko zmanjšali.

(2) Večji kibernetski incidenti lahko pomenijo sistemsko tveganje za finančni sistem, saj lahko povzročijo motnje kritičnih finančnih storitev in operacij. Začetni pretres se lahko okrepi s širjenjem operativnih ali finančnih škodljivih vplivov ali z upadanjem zaupanja v finančni sistem. Če finančni sistem ni zmožen absorbirati teh pretresov, to pomeni tveganje za finančno stabilnost in take razmere lahko vodijo do sistemske kibernetske krize ([5]).

([1]) UL L 1, 3.1.1994, str. 3.
([2]) UL L 331, 15.12.2010, str. 1.
([3]) UL C 58, 24.2.2011, str. 4.
([4]) Priporočilo ESRB/2013/1 Evropskega odbora za sistemska tveganja z dne 4. aprila 2013 o vmesnih ciljih in instrumentih makrobonitetne politike (UL C 170, 15.6.2013, str. 1).
([5]) Glej *Systemic cyber risk*, ESRB, februar 2020, dostopno na spletni strani ESRB na naslovu www.esrb.europa.eu.

(3) Nenehno razvijajoče se področje kibernetskih groženj in nedavno povečanje večjih kibernetskih incidentov sta pokazatelja večjega tveganja za finančno stabilnost v Uniji. Pandemija COVID-19 je izpostavila pomembnost tehnologije pri omogočanju delovanja finančnega sistema. Ustrezni organi in institucije so morali svojo tehnično infrastrukturo in okvire za upravljanje tveganj prilagoditi nenadnemu porastu dela na daljavo, kar je povečalo splošno izpostavljenost finančnega sistema kibernetskim grožnjam in omogočilo storilcem kaznivih dejanj, da odkrijejo nove načine delovanja in prilagodijo obstoječe ter tako izkoristijo razmere ([6]). Ob tem se je število kibernetskih incidentov, sporočenih bančnemu nadzoru ECB, v letu 2020 povečalo za 54 % v primerjavi z letom 2019 ([7]).

(4) Potencialno velik obseg, hitrost in stopnja širjenja večjega kibernetskega incidenta zahtevajo učinkovit odziv ustreznih organov, da se zmanjšajo morebitni negativni učinki na finančno stabilnost. Hitro usklajevanje in komuniciranje med ustreznimi organi na ravni Unije lahko pripomoreta k zgodnji oceni učinka večjega kibernetskega incidenta na finančno stabilnost, s čimer se ohrani zaupanje v finančni sistem in omeji širjenje škodljivih vplivov na druge finančne institucije ter tako prispeva k preprečevanju, da bi večji kibernetski incident pomenil tveganje za finančno stabilnost.

(5) Osnovni pretres se pojavi na način, ki je v primerjavi s tradicionalnimi finančnimi in likvidnostnimi krizami, s katerimi se običajno soočajo ustrezni organi, povsem nov. Poleg finančnih vidikov mora celotna ocena tveganja vključevati obseg in učinek operativnih motenj, saj bi lahko te vplivale na izbiro makrobonitetnih orodij. Finančna stabilnost bi lahko prav tako vplivala na to, katere ukrepe za zmanjševanje operativnega tveganja bodo izbrali strokovnjaki za kibernetsko varnost. To zahteva tesno in takojšnje usklajevanje ter odprto komuniciranje, da se med drugim izoblikuje situacijsko zavedanje.

(6) Tveganje neusklajevanja med organi obstaja in ga je treba obravnavati. Ustrezni organi v Uniji se bodo morali usklajevati med seboj in z drugimi organi, na primer z Agencijo Evropske unije za kibernetsko varnost (ENISA), s katerimi morda običajno ne sodelujejo. Ker znatno število finančnih institucij Unije posluje globalno, večji kibernetski incident verjetno ne bo omejen na Unijo ali bo lahko sprožen zunaj Unije in bo morda zahteval usklajevanje odzivov na globalni ravni.

(7) Ustrezni organi morajo biti pripravljeni na tako sodelovanje. V nasprotnem primeru bi se lahko pojavilo tveganje neskladnega ukrepanja, ki bi nasprotovalo odzivom drugih organov ali jih ogrozilo. Tako neusklajevanje bi lahko okrepilo pretres za finančni sistem in vodilo k upadu zaupanja v delovanje finančnega sistema, kar bi v najslabšem primeru pomenilo tveganje za finančno stabilnost ([8]). Zato bi bilo treba sprejeti ukrepe za obravnavanje tveganja za finančno stabilnost, ki izhaja iz neusklajevanja v primeru večjega kibernetskega incidenta.

(8) Poročilo ESRB „*Mitigating systemic cyber risk* (2021)“ ([9]) prepoznava potrebo po vzpostavitvi vseevropskega okvira za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF) za ustrezne organe v Uniji. Cilj EU-SCICF bi bil zvišati stopnjo pripravljenosti ustreznih organov, da se omogoči usklajen odziv na morebitni večji kibernetski incident. Navedeno poročilo vsebuje oceno ESRB o značilnostih okvira, ki bi bile verjetno potrebne za obravnavo tveganja neusklajevanja.

(9) Ključni cilj tega priporočila je nadgraditi eno od predvidenih vlog evropskih nadzornih organov na podlagi predloga uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor ([10]) (v nadaljnjem besedilu: uredba DORA), da postopoma omogočijo učinkovit usklajen odziv na ravni Unije v primeru večjega čezmejnega incidenta, povezanega z informacijsko in komunikacijsko tehnologijo (IKT), ali s tem povezane grožnje, ki bi imela sistemski učinek na celotni finančni sektor Unije. Ta proces bo privedel do vzpostavitve okvira EU-SCICF za ustrezne organe.

([6]) Glej *Internet Organised Crime Threat Assessment*, Europol, 2020, dostopno na spletni strani Europola na naslovu www.europol.europa.eu.
([7]) Glej *IT and cyber risk: a constant challenge*, ECB, 2021, dostopno na spletni strani bančnega nadzora ECB na naslovu www.bankingsupervision.europa.eu.
([8]) Glej *Systemic cyber risk*, ESRB, februar 2020, dostopno na spletni strani ESRB na naslovu www.esrb.europa.eu.
([9]) Glej *Mitigating systemic cyber risk*, ESRB, 2021 (še ni na razpolago).
([10]) COM/2020/595 final.

(10) EU-SCICF ne bi smel nadomestiti obstoječih okvirov, temveč premostiti vrzeli v usklajevanju in komuniciranju, ki obstajajo med ustreznimi organi samimi ter med ustreznimi organi in drugimi organi v Uniji in drugimi ključnimi akterji na mednarodni ravni. V tej zvezi je treba proučiti umestitev EU-SCICF v obstoječo ureditev okvira za ravnanje v finančni krizi in okvira Unije za kibernetske incidente. V zvezi z usklajevanjem med ustreznimi organi je treba med drugim proučiti vloge in dejavnosti skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov za finančne subjekte na podlagi Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([11]) ter mehanizme usklajevanje, predvidene z vzpostavitvijo skupne kibernetske enote, skupaj z udeležbo ENISA.

(11) Predlog za začetek priprave EU-SCICF je zlasti namenjen potrditvi morebitnih vlog evropskih nadzornih organov, kot jih predvideva predlog uredbe DORA. V uredbi DORA se predlaga, da lahko „evropski nadzorni organi […] prek Skupnega odbora in v sodelovanju s pristojnimi organi, ECB in ESRB vzpostavijo mehanizme, ki omogočajo izmenjavo učinkovitih praks med finančnimi sektorji za povečanje situacijskega zavedanja in prepoznavanje skupnih kibernetskih ranljivosti in tveganj med sektorji“, in „oblikujejo […] vaje za krizno upravljanje in izredne razmere, ki vključujejo scenarije kibernetskih napadov, da bi razvili komunikacijske kanale in postopoma omogočili učinkovit usklajen odziv na ravni EU v primeru večjega čezmejnega incidenta, povezanega z IKT, ali s tem povezane grožnje, ki bi imela sistemski učinek na celotni finančni sektor Unije“ ([12]). Vseevropski okvir, kakršen bi bil EU-SCICF, še ne obstaja in bi ga bilo treba vzpostaviti in razviti v kontekstu uredbe DORA.

(12) Glede na tveganje za finančno stabilnost v Uniji, ki izvira iz kibernetskega tveganja, bi se moralo pripravljalno delo za postopno vzpostavitev EU-SCICF začeti, kolikor je to izvedljivo, še preden se začne v celoti uporabljati pravni okvir in okvir politike, ki sta potrebna za njegovo vzpostavitev. Ta pravni okvir in okvir politike bi bila v celoti izdelana in dokončana do začetka uporabe ustreznih določb uredbe DORA in delegiranih aktov, sprejetih na njeni podlagi.

(13) Učinkovita komunikacija prispeva k situacijskemu zavedanju med ustreznimi organi in je zato nepogrešljiv pogoj za usklajevanje po vsej Uniji v času večjih kibernetskih incidentov. V tej zvezi bi bilo treba opredeliti komunikacijsko infrastrukturo, ki je potrebna za usklajevanje odziva na večji kibernetski incident. To bi zajemalo določitev vrste informacij, ki jih je treba izmenjati, ustaljenih kanalov, ki je treba uporabiti za izmenjavo teh informacij, in kontaktnih točk, s katerimi je treba informacije izmenjati. Pri izmenjavi informacij je treba upoštevati obstoječe pravne zahteve. Poleg tega bodo ustrezni organi morda morali opredeliti jasen akcijski načrt in protokole, po katerih bo treba ravnati, da se zagotovi ustrezno usklajevanje med organi, udeleženimi pri načrtovanju usklajenega odziva na večji kibernetski incident.

(14) Sistemska kibernetska kriza bo terjala zagon popolnega sodelovanja na nacionalni ravni in ravni Unije. Zato bo morda treba predvideti določitev kontaktnih točk pri evropskih nadzornih organih, ECB in vsaki državi članici med njihovimi ustreznimi nacionalnimi organi, ki bi jih bilo treba sporočiti evropskim nadzornim organom, da se določijo glavni sogovorniki v shemi usklajevanja EU-SCICF, ki se jih obvesti v primeru večjega kibernetskega incidenta. Potrebo po določitvi kontaktnih točk bi bilo treba oceniti med oblikovanjem EU-SCICF, ob upoštevanju imenovanih enotnih točk na podlagi Direktive (EU) 2016/1148, ki so jih države članice določile v zvezi z varnostjo omrežij in informacijskih sistemov, da se zagotovi čezmejno sodelovanje z drugimi državami članicami in skupino za sodelovanje na področju varnosti omrežij in informacijskih sistemov ([13]).

(15) Izvedba vaj za krizno upravljanje in izredne razmere bi lahko olajšala izvajanje EU-SCICF in omogočila organom, da ovrednotijo svojo pripravljenost na sistemsko kibernetsko krizo na ravni Unije. Take vaje bi organom zagotovile nova spoznanja in omogočile, da se EU-SCICF stalno izboljšuje in razvija.

([11]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

([12]) Glej osnutek člena 43 predloga uredbe DORA.

([13]) Glej Evropska komisija, *NIS Cooperation Group*, dostopno na spletni strani Evropske komisije na naslovu www.ec.europa.eu.

(16) Za razvoj EU-SCICF je bistveno, da evropski nadzorni organi skupaj opravijo ustrezno pripravljalno delo, da se proučijo potencialni ključni elementi okvira ter zahtevani viri in potrebe za nadaljevanje njegovega razvoja. Po tem bi lahko evropski nadzorni organi začeli izvajati predhodno analizo o ovirah, ki bi lahko okrnile zmožnosti evropskih nadzornih organov in ustreznih organov, da vzpostavijo EU-SCICF in si izmenjujejo ustrezne informacije po komunikacijskih kanalih v primeru večjega kibernetskega incidenta. Taka analiza bi bila pomemben korak k nadaljnjim ukrepom zakonodajne narave ali v obliki drugih podpornih pobud, ki jih lahko Evropska komisija sprejme po uveljavitvi uredbe DORA –

SPREJEL NASLEDNJE PRIPOROČILO:

ODDELEK 1

PRIPOROČILA

Priporočilo A – vzpostavitev vseevropskega okvira za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF)

1. Priporoča se, da se evropski nadzorni organi, kot je predvideno v predlogu Komisije za uredbo Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor (v nadaljnjem besedilu: uredba DORA), prek skupnega odbora in skupaj z Evropsko centralno banko (ECB), Evropskim odborom za sistemska tveganja (ESRB) in ustreznimi nacionalnimi organi začnejo pripravljati na postopno oblikovanje učinkovitega usklajenega odziva na ravni Unije v primeru večjega čezmejnega kibernetskega incidenta ali s tem povezane grožnje, ki bi lahko imela sistemski učinek na finančni sektor Unije. Pripravljalno delo za usklajen odziv na ravni Unije bi moralo obsegati postopno oblikovanje EU-SCICF za evropske nadzorne organe, ECB, ESRB in ustrezne nacionalne organe. Vključevati bi moralo tudi oceno potrebnih virov za učinkovito oblikovanje EU-SCICF.

2. Priporoča se, da evropski nadzorni organi z vidika podpriporočila A(1) po posvetovanju z ECB in ESRB ugotovijo in nato analizirajo sedanje ovire ter pravne in druge operativne prepreke za učinkovito oblikovanje EU-SCICF.

Priporočilo B – vzpostavitev kontaktnih točk EU-SCICF

Priporoča se, da evropski nadzorni organi, ECB in vsaka država članica med svojimi ustreznimi nacionalnimi organi določijo glavno kontaktno točko, ki jo je treba sporočiti evropskim nadzornim organom. Seznam kontaktnih točk bo olajšal oblikovanje okvira, po vzpostavitvi EU-SCICF pa bo treba kontaktne točke in ESRB obvestiti v primeru večjega kibernetskega incidenta. Predvideti bi bilo treba tudi sodelovanje med EU-SCICF in imenovanimi enotnimi kontaktnimi točkami na podlagi Direktive (EU) 2016/1148, ki so jih države članice določile v zvezi z varnostjo omrežij in informacijskih sistemov, da se zagotovi čezmejno sodelovanje z drugimi državami članicami in skupino za sodelovanje na področju varnosti omrežij in informacijskih sistemov.

Priporočilo C – ustrezni ukrepi na ravni Unije

Priporoča se, da Komisija na podlagi rezultatov analiz, izvedenih v skladu s priporočilom A, prouči ustrezne ukrepe, ki so potrebni za učinkovito usklajevanje odzivov na sistemske kibernetske incidente.

ODDELEK 2

IZVAJANJE

1. **Opredelitev pojmov**

V tem priporočilu se uporabljajo naslednje opredelitve pojmov:

(a) „kibernetski“ pomeni v zvezi z, znotraj ali prek medija medsebojno povezane informacijske infrastrukture, ki vključuje povezave med osebami, procesi, podatki in informacijskimi sistemi ([14]);

([14]) Glej *Cyber Lexicon*, Odbor za finančno stabilnost (FSB), 12. november 2018, dostopno na spletni strani FSB na naslovu www.fsb.org.

(b) „večji kibernetski incident“ pomeni incident, povezan z IKT, s potencialno velikim škodljivim učinkom na omrežje in informacijske sisteme, ki podpirajo kritične funkcije finančnih subjektov ([15]);

(c) „sistemska kibernetska kriza“ pomeni večji kibernetski incident, ki povzroči tako stopnjo motenj v finančnem sistemu Unije, ki lahko pomeni resne negativne posledice za nemoteno delovanje notranjega trga in realnega gospodarstva. Taka kriza lahko izhaja iz večjega kibernetskega incidenta, ki povzroči pretrese v številnih kanalih, vključno z operativnimi kanali, kanali zaupanja in finančnimi kanali;

(d) „evropski nadzorni organi“ pomeni Evropski nadzorni organ (Evropski bančni organ), ustanovljen z Uredbo (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([16]), skupaj z Evropskim nadzornim organom (Evropskim organom za zavarovanja in poklicne pokojnine), ustanovljenim z Uredbo (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([17]), in Evropskim nadzornim organom (Evropskim organom za vrednostne papirje in trge), ustanovljenim z Uredbo (EU) št. 1095/2010 Evropskega parlamenta in Sveta ([18]);

(e) „Skupni odbor “ pomeni Skupni odbor evropskih nadzornih organov, ustanovljen s členom 54 Uredbe (EU) št. 1093/2010, Uredbe (EU) št. 1094/2010 in Uredbe (EU) št. 1095/2010;

(f) „ustrezni nacionalni organ“ pomeni:

1. pristojni ali nadzorni organ v državi članici, kakor je določen v aktih Unije, navedenih v členu 1(2) Uredbe št. 1093/2010, Uredbe (EU) št. 1094/2010 in Uredbe (EU) št. 1095/2010, in kateri koli drugi pristojni nacionalni organ, kakor je določen v aktih Unije, ki podeljujejo naloge evropskim nadzornim organom;

2. pristojni organ v državni članici, imenovan v skladu s:

i. členom 4 Direktive 2013/36/EU Evropskega parlamenta in Sveta ([19]), brez poseganja v posebne naloge, ki so prenesene na ECB z Uredbo Sveta (EU) št. 1024/2013 ([20]);

ii. členom 22 Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta ([21]);

iii. členom 37 Direktive 2009/110/ES Evropskega parlamenta in Sveta ([22]);

iv. členom 4 Direktive (EU) 2019/2034 Evropskega parlamenta in Sveta ([23]);

([15]) Glej točko 7 osnutka člena 3 predloga uredbe DORA.

([16]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

([17]) Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48).

([18]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84).

([19]) Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

([20]) Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na Evropsko centralno banko (UL L 287, 29.10.2013, str. 63).

([21]) Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35).

([22]) Direktiva 2009/110/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja ter o spremembah direktiv 2005/60/ES in 2006/48/ES in razveljavitvi Direktive 2000/46/ES (UL L 267, 10.10.2009, str. 7).

([23]) Direktiva (EU) 2019/2034 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o bonitetnem nadzoru investicijskih podjetij ter o spremembi direktiv 2002/87/ES, 2009/65/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU in 2014/65/EU (UL L 314, 5.12.2019, str. 64).

v. prvo alineo točke (ee) člena 3(1) predloga Uredbe Evropskega parlamenta in Sveta o trgih kriptoimetij in spremembi Direktive (EU) 2019/1937 ([24]);

vi. členom 11 Uredbe (EU) št. 909/2014 Evropskega parlamenta in Sveta ([25]);

vii. členom 22 Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ([26]);

viii. členom 67 Direktive 2014/65/EU Evropskega parlamenta in Sveta ([27]);

ix. členom 22 Uredbe (EU) št. 648/2012;

x. členom 44 Direktive 2011/61/EU Evropskega parlamenta in Sveta ([28]);

xi. členom 97 Direktive 2009/65/ES Evropskega parlamenta in Sveta ([29]);

xii. členom 30 Direktive 2009/138/ES Evropskega parlamenta in Sveta ([30]);

xiii. členom 12 Direktive (EU) 2016/97 Evropskega parlamenta in Sveta ([31]);

xiv. členom 47 Direktive (EU) 2016/2341 Evropskega parlamenta in Sveta ([32]);

xv. členom 22 Uredbe (EC) št. 1060/2009 Evropskega parlamenta in Sveta ([33]);

xvi. členom 3(2) in členom 32 Direktive 2006/43/ES Evropskega parlamenta in Sveta ([34]);

xvii. členom 40 Uredbe (EU) 2016/1011 Evropskega parlamenta in Sveta ([35]);

xviii. členom 29 Uredbe (EU) 2020/1503 Evropskega parlamenta in Sveta ([36]);

([24]) COM/2020/593 final.
([25]) Uredba (EU) št. 909/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah ter o spremembi direktiv 98/26/ES in 2014/65/EU ter Uredbe (EU) št. 236/2012 (UL L 257, 28.8.2014, str. 1).
([26]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).
([27]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).
([28]) Direktiva 2011/61/EU Evropskega parlamenta in Sveta z dne 8. junija 2011 o upraviteljih alternativnih investicijskih skladov in spremembah direktiv 2003/41/ES in 2009/65/ES ter uredb (ES) št. 1060/2009 in (EU) št. 1095/2010 (UL L 174, 1.7.2011, str. 1).
([29]) Direktiva 2009/65/ES Evropskega parlamenta z dne 13. julija 2009 o usklajevanju zakonov in drugih predpisov o kolektivnih naložbenih podjemih za vlaganja v prenosljive vrednostne papirje (KNPVP) (UL L 302, 17.11.2009, str. 32).
([30]) Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).
([31]) Direktiva (EU) 2016/97 Evropskega parlamenta in Sveta z dne 20. januarja 2016 o distribuciji zavarovalnih produktov (UL L 26, 2.2.2016, str. 19).
([32]) Direktiva (EU) 2016/2341 Evropskega parlamenta in Sveta z dne 14. decembra 2016 o dejavnostih in nadzoru institucij za poklicno pokojninsko zavarovanje (UL L 354, 23.12.2016, str. 37).
([33]) Uredba (ES) št. 1060/2009 Evropskega parlamenta in Sveta z dne 16. septembra 2009 o bonitetnih agencijah (UL L 302, 17.11.2009, str. 1).
([34]) Direktiva 2006/43/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o obveznih revizijah za letne in konsolidirane računovodske izkaze, spremembi direktiv Sveta 78/660/EGS in 83/349/EGS ter razveljavitvi Direktive Sveta 84/253/EGS (UL L 157, 9.6.2006, str. 87).
([35]) Uredba (EU) 2016/1011 Evropskega parlamenta in Sveta z dne 8. junija 2016 o indeksih, ki se uporabljajo kot referenčne vrednosti v finančnih instrumentih in finančnih pogodbah ali za merjenje uspešnosti investicijskih skladov, in spremembi direktiv 2008/48/ES in 2014/17/EU ter Uredbe (EU) št. 596/2014 (UL L 171, 29.6.2016, str. 1).
([36]) Uredba (EU) 2020/1503 Evropskega parlamenta in Sveta z dne 7. oktobra 2020 o evropskih ponudnikih storitev množičnega financiranja za podjetnike ter spremembi Uredbe (EU) 2017/1129 in Direktive (EU) 2019/1937 (UL L 347, 20.10.2020, str. 1).

3. organ, ki je pristojen za sprejetje in/ali aktiviranje ukrepov makrobonitetne politike ali za opravljanje drugih nalog v zvezi s finančno stabilnostjo, na primer za zagotavljanje s tem povezanih podpornih analiz, med drugim:

   i. imenovani organ v skladu s poglavjem 4 naslova VII Direktive 2013/36/EU ali členom 458(1) Uredbe Evropskega parlamenta in Sveta (EU) št. 575/2013 ([37]);

   ii. makrobonitetni organ s cilji, ureditvami, nalogami, pooblastili, instrumenti, zahtevami glede odgovornosti in drugimi značilnostmi, določenimi v Priporočilu ESRB/2011/3 Evropskega odbora za sistemska tveganja ([38]);

(g) „ustrezni organ“ pomeni:

1. evropski nadzorni organ;

2. ECB za naloge, ki so nanjo prenesene v skladu s členom 4(1) in (2) ter členom 5(2) Uredbe (EU) št. 1024/2013;

3. ustrezni nacionalni organ.

2. **Merila za izvajanje**

Za izvajanje tega priporočila se uporabljajo naslednja merila:

(a) treba je upoštevati načelo potrebe po seznanitvi in načelo sorazmernosti, ob upoštevanju cilja in vsebine vsakega priporočila;

(b) v zvezi z vsakim priporočilom je treba izpolniti posebna merila za skladnost, ki so določena v Prilogi.

3. **Časovni okvir za nadaljnje ukrepanje**

V skladu s členom 17(1) Uredbe (EU) št. 1092/2010 morajo naslovniki Evropski parlament, Svet, Komisijo in ESRB obvestiti, katere ukrepe so sprejeli na podlagi tega priporočila, ali utemeljiti vsako neukrepanje. Naslovniki navedeno obveščanje izvedejo po naslednjem časovnem razporedu:

1. Priporočilo A

(a) Do 30. junija 2023, vendar najhitreje šest mesecev po začetku veljavnosti uredbe DORA, evropski nadzorni organi predložijo Evropskemu parlamentu, Svetu, Komisiji in ESRB vmesno poročilo o izvajanju podpriporočila A(1).

(b) Do 30. junija 2024, vendar najhitreje 18 mesecev po začetku veljavnosti uredbe DORA, evropski nadzorni organi predložijo Evropskemu parlamentu, Svetu, Komisiji in ESRB končno poročilo o izvajanju podpriporočila A(1).

(c) Do 30. junija 2025, vendar najhitreje 30 mesecev po začetku veljavnosti uredbe DORA, evropski nadzorni organi predložijo Evropskemu parlamentu, Svetu, Komisiji in ESRB poročilo o izvajanju podpriporočila A(2).

2. Priporočilo B

Do 30. junija 2023, vendar najhitreje šest mesecev po začetku veljavnosti uredbe DORA, evropski nadzorni organi, ECB in države članice predložijo Evropskemu parlamentu, Svetu, Komisiji in ESRB poročilo o izvajanju priporočila B.

3. Priporočilo C

(a) Do 31. decembra 2023, vendar najhitreje 12 mesecev po začetku veljavnosti uredbe DORA, Komisija predloži Evropskemu parlamentu, Svetu in ESRB poročilo o izvajanju priporočila C glede na vmesno poročilo evropskih nadzornih organov v skladu s podpriporočilom A(1).

([37]) Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

([38]) Priporočilo ESRB/2011/3 Evropskega odbora za sistemska tveganja z dne 22. decembra 2011 o makrobonitetnem mandatu nacionalnih organov (UL C 41, 14.2.2012, str. 1).

(b) Do 31. decembra 2025, vendar najhitreje 36 mesecev po začetku veljavnosti uredbe DORA, Komisija predloži Evropskemu parlamentu, Svetu in ESRB poročilo o izvajanju priporočila C glede na poročila evropskih nadzornih organov v skladu s priporočilom A.

4. **Spremljanje in ocenjevanje**

1. Sekretariat ESRB:

(a) nudi pomoč naslovnikom z zagotavljanjem koordiniranega poročanja in ustreznih predlog ter, kjer je potrebno, podrobnejšim določanjem postopka in časovnega okvira za nadaljnje ukrepanje;

(b) preverja nadaljnje ukrepanje naslovnikov in jim nudi pomoč, če zanjo zaprosijo, ter splošnemu odboru predloži poročila o nadaljnjem ukrepanju. Uvedli se bodo naslednji postopki ocenjevanja:

(i) v 12 mesecih po začetku veljavnosti uredbe DORA v zvezi z izvajanjem priporočil A in B;

(ii) v 18 mesecih po začetku veljavnosti uredbe DORA v zvezi z izvajanjem priporočila C;

(iii) v 24 mesecih po začetku veljavnosti uredbe DORA v zvezi z izvajanjem priporočila A;

(iv) v 36 mesecih po začetku veljavnosti uredbe DORA v zvezi z izvajanjem priporočila A;

(v) v 42 mesecih po začetku veljavnosti uredbe DORA v zvezi z izvajanjem priporočila C;

2. Splošni odbor oceni ukrepe in utemeljitve, ki jih sporočijo naslovniki, ter lahko, kjer je primerno, presodi, da to priporočilo ni bilo upoštevano in naslovnik ni ustrezno utemeljil, zakaj ni ukrepal.

V Frankfurtu na Majni, 2. decembra 2021

Vodja sekretariata ESRB
V imenu splošnega odbora ESRB
Francesco MAZZAFERRO

PRILOGA

DOLOČITEV MERIL ZA SKLADNOST, KI SE UPORABLJAJO ZA PRIPOROČILA

Priporočilo A – vzpostavitev vseevropskega okvira za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF)

Za podpriporočilo A(1) se uporabljajo naslednja merila za skladnost.

1. Pri pripravi učinkovitega usklajenega odziva na ravni Unije, ki bi morala obsegati postopno oblikovanje EU-SCICF z izvrševanjem pooblastil, predvidenih v prihodnji uredbi Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor (v nadaljnjem besedilu: uredba DORA), bi morali evropski nadzorni organi prek skupnega odbora skupaj z Evropsko centralno banko (ECB), Evropskim odborom za sistemska tveganja (ESRB) in ustreznimi nacionalni organi ter po posvetovanju z Agencijo Evropske unije za kibernetsko varnost in Komisijo, kjer je to potrebno, proučiti možnost, da se v predvideno pripravo EU-SCICF vključijo vsaj naslednji vidiki:

   a. analiza potrebnih virov za učinkovito oblikovanje EU-SCICF;

   b. oblikovanje vaj za krizno upravljanje in izredne razmere, ki vključujejo scenarije kibernetskih napadov, da bi razvili komunikacijske kanale;

   c. oblikovanje skupnega besedišča;

   d. oblikovanje skladne razvrstitve kibernetskih incidentov;

   e. vzpostavitev varnih in zanesljivih kanalov za izmenjavo informacij, vključno z rezervnimi sistemi;

   f. določitev kontaktnih točk;

   g. obravnava zaupnosti pri izmenjavi informacij;

   h. pobude za sodelovanje in izmenjavo informacij s kibernetsko obveščevalno službo za finančni sektor;

   i. vzpostavitev učinkovitih procesov za aktiviranje in prenos na višjo raven na podlagi situacijskega zavedanja;

   j. razjasnitev odgovornosti udeležencev okvira;

   k. oblikovanje vmesnikov za usklajevanje med sektorji in, kjer je primerno, s tretjimi državami;

   l. zagotovitev usklajene komunikacije ustreznih organov z javnostjo, da se ohrani zaupanje;

   m. vzpostavitev vnaprej opredeljenih komunikacijskih kanalov za pravočasno komunikacijo;

   n. izvedba ustreznih vaj za testiranje okvira, vključno s testiranjem med jurisdikcijami in usklajevanjem s tretjimi državami, in ocen, ki privedejo do novih spoznanj in razvoja okvira;

   o. zagotovitev učinkovite komunikacije in ukrepov proti dezinformacijam.

Priporočilo B – vzpostavitev kontaktnih točk EU-SCICF

Za priporočilo B se uporabljata naslednji merili za skladnost.

1. Evropski nadzorni organi, ECB in vsaka država članica med svojimi ustreznimi nacionalnimi organi bi se morali dogovoriti o skupnem pristopu k izmenjavi in posodabljanju seznama določenih kontaktnih točk EU-SCICF.

2. Določitev kontaktne točke bi se morala presojati ob upoštevanju imenovanih enotnih kontaktnih točk na podlagi Direktive (EU) 2016/1148, ki so jih države članice določile v zvezi z varnostjo omrežij in informacijskih sistemov, da se zagotovi čezmejno sodelovanje z drugimi državami članicami in skupino za sodelovanje na področju varnosti omrežij in informacijskih sistemov.

Priporočilo C –spremembe pravnega okvira Unije

Za priporočilo C se uporablja naslednje merilo za skladnost.

Komisija bi morala proučiti, ali so na podlagi analize, izvedene v skladu s priporočilom A potrebni kakršni koli ukrepi, vključno s spremembami ustrezne zakonodaje Unije, da se zagotovi, da lahko evropski nadzorni organi prek skupnega odbora ter skupaj z ECB, ESRB in ustreznimi nacionalnimi organi oblikujejo EU-SCICF v skladu s podpriporočilom A(1), in da se omogoči, da lahko evropski nadzorni organi, ECB, ESRB, ustrezni nacionalni organi in drugi organi sodelujejo pri usklajevanju in si izmenjujejo informacije, ki so dovolj podrobne in skladne za podporo učinkovitemu EU-SCICF.