III.

(Pripremni akti)

EUROPSKA SREDIŠNJA BANKA

MIŠLJENJE EUROPSKE SREDIŠNJE BANKE

od 4. lipnja 2021.

o Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor

(CON/2021/20)

(2021/C 343/01)

Uvod i pravna osnova

Europska središnja banka (ESB) zaprimila je 22., 23. i 29. prosinca 2020. zahtjeve Vijeća Europske unije i Europskog parlamenta za davanje mišljenja o Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014 ([1]) (dalje u tekstu „Prijedlog uredbe") i Prijedlogu direktive o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EZ, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 i (EU) 2016/2341 ([2]) (dalje u tekstu „Prijedlog direktive o izmjeni", zajedno s „Prijedlogom uredbe" „prijedlozi akata").

Nadležnost ESB-a za davanje mišljenja temelji se na članku 127. stavku 4. i članku 282. stavku 5. Ugovora o funkcioniranju Europske unije, s obzirom na to da prijedlozi akata sadrže odredbe iz područja nadležnosti ESB-a, a posebno određivanje i provedbu monetarne politike, promicanje nesmetanog funkcioniranja platnih sustava, doprinos nesmetanom vođenju politika koje provode nadležna tijela u vezi sa stabilnošću sustava financijskog tržišta te zadaća ESB-a u vezi s bonitetnim nadzorom kreditnih institucija u skladu s člankom 127. stavkom 2. prvom i četvrtom alinejom, člankom 127 stavkom 5. i člankom 127. stavkom 6. Ugovora. Upravno vijeće donijelo je ovo Mišljenje u skladu s prvom rečenicom članka 17. stavka 5. Poslovnika Europske središnje banke.

1. Opće napomene

1.1 ESB pozdravlja Prijedlog uredbe čiji je cilj jačanje kibersigurnosti i operativne otpornosti financijskog sektora. ESB posebno pozdravlja cilj Prijedloga uredbe da se uklone prepreke i unaprijedi uspostava i funkcioniranje unutarnjeg tržišta financijskih usluga usklađivanjem pravila koja se primjenjuju u području upravljanja rizicima informacijske i komunikacijske tehnologije (IKT), izvješćivanja, testiranja i IKT rizikom treće strane. Nadalje, ESB pozdravlja cilj Prijedloga uredbe da se racionaliziraju i usklade svi regulatorni zahtjevi koji se preklapaju ili nadzorna očekivanja kojima financijski subjekti trenutačno podliježu u skladu s pravom Unije.

1.2 ESB razumije da Prijedlog uredbe predstavlja, u odnosu na financijske subjekte identificirane kao operatore ključnih usluga ([3]), zakonodavstvo vezano za određeni sektor (*lex specialis*) u skladu sa značenjem iz članka 1. stavka 7. Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća ([4]) (dalje u tekstu „Direktiva NIS"); što znači da bi zahtjevi iz Prijedloga uredbe u načelu imali prednost pred Direktivom NIS. U praksi bi financijski subjekti koji su identificirani kao operatori ključnih usluga ([5]), među ostalim, prijavili incidente u skladu s Prijedlogom

([1]) COM(2020) 595 konačno.
([2]) COM(2020) 596 konačno.
([3]) Vidi članak 1. stavak 2. Prijedloga uredbe.
([4]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).
([5]) Vidi članak 5. Direktive NIS.

uredbe, a ne Direktivom NIS. Iako ESB pozdravlja smanjenje mogućih preklapanja zahtjeva za financijske subjekte u području izvješćivanja o incidentima, trebalo bi dodatno razmotriti međudjelovanje Prijedloga uredbe i Direktive NIS. Primjerice, na temelju Prijedloga uredbe na treću stranu pružatelja IKT usluga ([6]) mogle bi se primjenjivati preporuke koje donosi glavno nadzorno tijelo ([7]). Istodobno, ista treća strana pružatelj IKT usluga može se klasificirati kao operator ključnih usluga u skladu s Direktivom NIS i podliježe obvezujućim uputama koje donosi nadležno tijelo ([8]). U tom bi slučaju treća strana pružatelj IKT usluga mogla podlijegati proturječnim preporukama donesenima u skladu s Prijedlogom uredbe i obvezujućim uputama donesenima u skladu s Direktivom NIS. ESB predlaže da zakonodavna tijela Unije dodatno razmotre moguće nedosljednosti između Prijedloga uredbe i Direktive NIS koje bi mogle ometati usklađivanje te smanjenje preklapanja i proturječne zahtjeve za financijske subjekte.

1.3 ESB također razumije da će u skladu s Prijedlogom direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije kojom se stavlja izvan snage Direktiva (EU) 2016/1148 ([9]) (dalje u tekstu „Prijedlog direktive NIS2"), „izbjegnuti incidenti" ([10]) podlijegati obvezama izvješćivanja ([11]). Iako se u uvodnoj izjavi 39. Prijedloga direktive NIS2 upućuje na značenje pojma „izbjegnuti incidenti", nije jasno namjerava li se zahtijevati da financijski subjekti navedeni u članku 2. Prijedloga uredbe izvješćuju o izbjegnutim incidentima. U tom pogledu i uzimajući u obzir da se izbjegnuti incidenti mogu identificirati kao takvi tek nakon što do njih dođe, ESB bi pozdravio pravodobno primanje obavijesti o važnim izbjegnutim incidentima, kao što je trenutačno slučaj s kiberincidentima. ESB predlaže veću usklađenost između Prijedloga uredbe i Prijedloga direktive NIS2 kako bi se razjasnio točan opseg izvješćivanja kojem bilo koji financijski subjekt može podlijegati na temelju tih dvaju različitih, ali povezanih zakonodavnih akata Unije. Istodobno bi trebalo definirati „izbjegnute incidente" i razraditi odredbe kojima se pojašnjava njihova važnost.

1.4 ESB pozdravlja poticanje financijskih subjekata da na dobrovoljnoj osnovi međusobno razmjenjuju obavještajne informacije kako bi unaprijedili i ojačali svoje stavove o kiberotpornosti. Sam ESB pomogao je inicijativom za razmjenu obavještajnih informacija o kibrerprijetnjama (CIISI-EU) utemeljenom na potrebama tržišta i stavio je na raspolaganje nacrte za izradu i jačanje takve inicijative ([12]).

1.5 ESB podupire suradnju između nadležnih tijela za potrebe Prijedloga uredbe, europskih nadzornih tijela i timova za odgovor na računalne sigurnosne incidente (CSIRTS) ([13]). Ključno je razmjenjivati informacije kako bi se osigurala operativna otpornost Unije jer se razmjenom informacija i suradnjom među tijelima može doprinijeti sprečavanju kibernapada i smanjenju širenja IKT prijetnji. Trebalo bi promicati opće razumijevanje IKT rizika i osigurati dosljednu procjenu takvih rizika u cijeloj Uniji. Iznimno je važno da nadležna tijela razmjenjuju informacije s jedinstvenom kontaktnom točkom ([14]) i nacionalnim CSIRTS-om ([15]) samo ako postoje jasno utvrđeni mehanizmi klasifikacije i razmjene informacija, zajedno s odgovarajućim zaštitnim mjerama za osiguravanje povjerljivosti.

1.6 Naposljetku, ESB bi pozdravio uvođenje pravila o osobnim podacima i čuvanju podataka u okviru Prijedloga uredbe. Trajanje razdoblja čuvanja podataka trebalo bi uzeti u obzir istragu, inspekciju, zahtjev za davanje informacija, komunikaciju, objavu, evaluaciju, provjeru, procjenu i izradu planova nadzora ili supervizije koje će nadležna tijela možda morati provesti u okviru svojih obveza i dužnosti u skladu s Prijedlogom uredbe. U tom bi pogledu bilo primjereno razdoblje čuvanja od 15 godina. To bi se razdoblje čuvanja

([6]) Vidi članak 3. stavak 15. Prijedloga uredbe.
([7]) Vidi članak 31. stavak 1. točku (d) Prijedloga uredbe.
([8]) Vidi članak 15. stavak 3. Direktive NIS.
([9]) COM(2020) 823 konačno.
([10]) Događaji koji su potencijalno mogli prouzročiti štetu, ali su uspješno spriječeni u potpunom ostvarenju; vidi uvodnu izjavu 39. Direktive NIS2.
([11]) Vidi članak 11. Direktive NIS2.
([12]) Inicijativa za razmjenu obavještajnih informacija o kiberprijetnjama (CIISI-EU) dostupna je na mrežnim stranicama ESB-a www.ecb.europa.eu.
([13]) Vidi članak 42. Prijedloga uredbe.
([14]) Vidi članak 8. stavak 3. Direktive NIS.
([15]) Vidi također članke 11., 26. i 27. Direktive NIS2.

podataka moglo skratiti ili produljiti, kao što to zahtijevaju posebni slučajevi. U tom pogledu ESB predlaže da zakonodavna tijela Unije pri formuliranju odgovarajuće odredbe o osobnim podacima i čuvanju podataka uzmu u obzir i načelo smanjenja količine podataka, kao i daljnju obradu u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe ([16]).

2. **Posebna opažanja o nadzoru te poravnanju i namiri vrijednosnih papira**

2.1 *Nadzorne nadležnosti ESSB-a i Eurosustava*

2.1.1 Usko povezani s njihovim osnovnim zadaćama monetarne politike, Ugovorom i Statutom Europskog sustava središnjih banaka i Europske središnje banke (dalje u tekstu: Statut ESSB-a) predviđa se da Eurosustav provodi nadzor nad sustavima poravnanja i namire. U skladu s četvrtom alinejom članka 127. stavka 2. Ugovora, što se ogleda u članku 3. stavku 1. Statuta, jedna od temeljnih zadaća Europskog sustava središnjih banaka (ESSB) je promicanje nesmetanog funkcioniranja platnih sustava. U izvršavanju ove osnovne zadaće, ESB i nacionalne središnje banke mogu stvoriti mogućnosti, a ESB može donositi propise radi osiguranja učinkovitih i pouzdanih sustava poravnanja i platnih sustava u Uniji i s drugim zemljama ([17]). U skladu sa svojom nadzornom ulogom, ESB je donio Uredbu (EU) br. 795/2014 Europske središnje banke (ESB/2014/28) (dalje u tekstu „Uredba o SIPS-u") ([18]). Uredbom o SIPS-u provode se, u propisanom obliku, Načela za infrastrukture financijskih tržišta iz travnja 2012. koja su izdali Odbor za platni sustav i sustav namire i Međunarodna organizacija komisija za vrijednosne papire ([19]), koja su pravno obvezujuća i obuhvaćaju sustave velikih plaćanja i platne sustave za mala plaćanja od sistemske važnosti kojima upravlja središnja banka Eurosustava ili privatni subjekt. Okvir nadzorne politike Eurosustava ([20]) utvrđuje platne instrumente kao „sastavni dio platnih sustava" i tako ih uključuje u opseg svog nadzora. Nadzorni okvir za platne instrumente trenutačno se preispituje ([21]). U tom okviru platni instrument (npr. kartica, kreditni transfer, izravno terećenje, prijenos elektroničkog novca i digitalni token za plaćanje ([22])) definira se kao personalizirani uređaj (ili skup uređaja) i/ili skup postupaka dogovorenih između korisnika platnih usluga i pružatelja platnih usluga koji se upotrebljavaju za iniciranje prijenosa vrijednosti ([23]).

2.1.2 S obzirom na navedeno, ESB pozdravlja isključivanje iz članka o području primjene Prijedloga uredbe upravitelja sustava kako je definiran u članku 2. točki (p) Direktive 98/26/EZ Europskog parlamenta i Vijeća ([24]), platnih sustava (uključujući one kojima upravljaju središnje banke), platnih shema i platnih

([16]) Vidi članak 4. točku (b) Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

([17]) Vidi članak 22. Statuta ESSB-a.

([18]) Uredba (EU) br. 795/2014 Europske središnje banke od 3. srpnja 2014. o nadzornim zahtjevima za sistemski važne platne sustave (ESB/2014/28) (SL L 217, 23.7.2014., str. 16.).

([19]) Dostupno na mrežnim stranicama Banke za međunarodne namire www.bis.org.

([20]) Okvir nadzorne politike Eurosustava, revidirana verzija (srpanj 2016.) dostupno na mrežnim stranicama ESB-a www.ecb.europa.eu.

([21]) Vidi revidirani konsolidirani nadzorni okvir Eurosustava za elektroničke platne instrumente, sheme i aranžmane iz listopada 2020. (okvir PISA), dostupno na mrežnim stranicama ESB-a www.ecb.europa.eu.

([22]) Digitalni token za plaćanje digitalni je prikaz vrijednosti osigurane potraživanjima ili imovinom koji se bilježe drugdje i koji omogućuje prijenos vrijednosti među krajnjim korisnicima. Ovisno o temeljnom obliku, digitalni tokeni za plaćanje mogu predvidjeti prijenos vrijednosti bez nužnog uključivanja središnje treće strane i/ili upotrebe računa za plaćanje.

([23]) „Prijenos vrijednosti". „Radnja prijenosa novčanih sredstava ili digitalnih tokena za plaćanje, koju inicira platitelj ili primatelj plaćanja u ime platitelja, ili polaganja ili podizanja gotovine na račun korisnika ili s njega, bez obzira na osnovne obveze između platitelja i primatelja plaćanja. Prijenos može uključivati jednog pružatelja platnih usluga ili više njih." Ova definicija „prijenosa vrijednosti" u okviru PISA-e odstupa od definicije prijenosa „novčanih sredstava" iz Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35.). „Prijenos vrijednosti" u kontekstu „platnog instrumenta" kako je definiran u toj Direktivi može se odnositi samo na prijenos „novčanih sredstava". U skladu s tom Direktivom, „novčana sredstva" ne uključuju digitalne tokene za plaćanje, osim ako se tokeni mogu razvrstati kao elektronički novac (ili hipotetski kao knjižni novac).

([24]) Direktiva 98/26/EZ Europskog parlamenta i Vijeća od 19. svibnja 1998 o konačnosti namire u platnim sustavima i sustavima za namiru vrijednosnih papira (SL L 166, 11.6.1998., str. 45.).

aranžmana s obzirom na primjenu prethodno navedenih nadzornih okvira. Zbog tih razloga, nadležnosti ESSB-a na temelju Ugovora i nadležnosti Eurosustava na temelju Uredbe o SIPS-u trebale bi biti jasno navedene u uvodnim izjavama Prijedloga uredbe.

2.1.3 Isto tako, ESB pozdravlja isključivanje iz primjene nadzornog okvira iz Prijedloga uredbe trećih strana pružatelja IKT usluga koji podliježu nadzornim okvirima uspostavljenima za potrebe podupiranja zadaća iz članka 127. stavka 2. Ugovora ([25]). U tom pogledu, ESB želi naglasiti da središnje banke ESSB-a koje djeluju u svojstvu monetarne vlasti ([26]) i Eurosustav kada pruža usluge putem sustava TARGET2, TARGET2-Securites (T2S) ([27]) i namire trenutačnih plaćanja u sustavu TARGET (TIPS) ([28]) ne podliježu članku o području primjene Prijedloga uredbe niti se mogu smatrati trećim stranama pružateljima IKT usluga te tako potencijalno klasificirati kao treće strane pružatelji ključnih IKT usluga za potrebe Prijedloga uredbe. Eurosustav nadzire T2S u vezi sa svojom nadležnošću da osigura učinkovite i pouzdane sustave poravnanja i platne sustave. Nadalje, ESMA je pojasnila da T2S nije pružatelj ključnih usluga ([29]) u smislu Uredbe (EU) br. 909/2014 Europskog parlamenta i Vijeća ([30]) (dalje u tekstu „Uredba o CSD-u"). Kao rezultat toga, organizacijska i operativna sigurnost, učinkovitost i otpornost sustava T2S osiguravaju se primjenjivim pravnim, regulatornim i operativnim okvirom i dogovorenim sustavima upravljanja ili sustavom T2S, a ne kroz Uredbu o CSD-u.

2.1.4 Osim toga, okvirom nadzorne politike Eurosustava ([31]) obuhvaćeni su pružatelji ključnih usluga kao što je Društvo za svjetsku međubankovnu financijsku telekomunikaciju (*Society for Worldwide Interbank Financial Telecommunication*) (SWIFT). SWIFT je zadruga s ograničenom odgovornošću sa sjedištem u Belgiji, koja pruža usluge sigurnog prijenosa poruka na međunarodnoj razini. Nationale Bank van België/Banque Nationale de Belgique djeluje kao glavno nadzorno tijelo SWIFT-a i na temelju sporazuma o nadzoru zadruga provodi nadzor nad SWIFT-om u suradnji s drugim središnjim bankama skupine G10, uključujući ESB. Nadzorna tijela skupine G10 priznaju da je glavni fokus nadzora operativni rizik SWIFT-a jer se to smatra primarnom kategorijom rizika u okviru koje bi SWIFT mogao predstavljati sistemski rizik za financijski sustav u Uniji. U tom je pogledu Skupina za nadzor zadruge SWIFT (*SWIFT Cooperative Oversight Group*) razvila poseban skup načela i očekivanja visoke razine koji se primjenjuju na SWIFT, kao što su utvrđivanje rizika i upravljanje njime, informacijska sigurnost, pouzdanost i otpornost, tehnološko planiranje i komunikacija s korisnicima. Nadzorna tijela skupine G10 očekuju da se SWIFT pridržava smjernica Odbora za plaćanja i tržišne infrastrukture (CPMI) i Međunarodne organizacije komisija za vrijednosne papire (IOSCO) o kiberotpornosti ([32]), kao i drugih međunarodnih standarda o sigurnosti IKT-a koji, kad se promatraju zajedno, premašuju zahtjeve utvrđene u Prijedlogu uredbe.

2.1.5 Nije sigurno da bi SWIFT i možda drugi pružatelji usluga koji podliježu okviru nadzorne politike Eurosustava mogli podlijegati Prijedlogu uredbe kao treće strane pružatelji IKT usluga ako bi pružali usluge koje nisu obuhvaćene člankom 127. stavkom 2. Ugovora. ESB stoga snažno pozdravlja to što su pružatelji usluga koji već podliježu okviru nadzorne politike Eurosustava, uključujući, ali ne ograničavajući se na SWIFT, isključeni iz područja primjene nadzornog okvira utvrđenog u Prijedlogu uredbe.

([25]) Vidi članak 28. stavak 5. Prijedloga uredbe.

([26]) Vidi stavak 1.3 Mišljenja Europske središnje banke od 19. veljače 2021. o Prijedlogu uredbe o tržištima kriptoimovine i izmjeni Direktive (EU) 2019/1937 (CON/2021/4). Sva mišljenja ESB-a objavljuju su na EUR-Lexu.

([27]) Vidi Prilog II.a Smjernici ESB/2012/27 Europske središnje banke od 5. prosinca 2012. o Transeuropskom automatiziranom sustavu ekspresnih novčanih transakcija u realnom vremenu na bruto načelu (sustav TARGET2) (SL L 30, 30.1.2013., str. 1.). Smjernica ESB/2021/13 Europske središnje banke od 18. srpnja 2012. o sustavu TARGET2-Securities (SL L 215, 11.8.2012., str. 19.); Odluka ESB/2011/20 Europske središnje banke od 16. studenoga 2011. o utvrđivanju detaljnih pravila i postupaka za provođenje kriterija prihvatljivosti središnjih depozitorija vrijednosnih papira za pristup uslugama sustava TARGET2-Securities (SL L 319, 2.12.2011., str. 117.). Vidi također Okvirni sporazum sustava T2S i kolektivni ugovor.

([28]) Vidi Prilog II.b Smjernici ESB/2012/27.

([29]) Vidi članak 30. stavak 5. Uredbe (EU) br. 909/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o poboljšanju namire vrijednosnih papira u Europskoj uniji i o središnjim depozitorijima vrijednosnih papira te izmjeni direktiva 98/26/EZ i 2014/65/EU te Uredbe (EU) br. 236/2012 (SL L 257, 28.8.2014., str. 1.) i članak 68. Delegirane uredbe Komisije (EU) 2017/392 od 11. studenoga 2016. o dopuni Uredbe (EU) br. 909/2014 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda povezanih sa zahtjevima za odobrenje za rad te nadzornim i operativnim zahtjevima za središnje depozitorije vrijednosnih papira (SL L 65, 10.3.2017., str. 48.).

([30]) Uredba (EU) br. 909/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o poboljšanju namire vrijednosnih papira u Europskoj uniji i o središnjim depozitorijima vrijednosnih papira te izmjeni direktiva 98/26/EZ i 2014/65/EU te Uredbe (EU) br. 236/2012 (SL L 257, 28.8.2014., str. 1.).

([31]) Okvir nadzorne politike Eurosustava, revidirana inačica (srpanj 2016.) dostupno na mrežnim stranicama ESB-a www.ecb.europa.eu.

([32]) Dostupno na mrežnim stranicama Banke za međunarodne namire www.bis.org.

2.2 *Nadležnosti ESSB-a u području namire vrijednosnih papira*

2.2.1 Središnji depozitoriji vrijednosnih papira su infrastrukture financijskog tržišta koje su strogo regulirane i koje nadziru različita tijela u skladu s Uredbom o CSD-u kojom se utvrđuju zahtjevi za namiru financijskih instrumenata te pravila o organizaciji i ponašanju središnjih depozitorija vrijednosnih papira. Nadalje, središnji depozitoriji vrijednosnih papira trebaju uzeti u obzir Smjernice CPMI-IOSCO o kiberotpornosti, koje su razrađene Nadzornim očekivanjima povezanim s kiberotpornošću za infrastrukture financijskog tržišta (prosinac 2018.) ([33]). Osim nadzornih ovlasti povjerenih nacionalnim nadležnim tijelima u skladu s Uredbom o CSD-u, članovi ESSB-a djeluju kao „relevantna tijela", u svojstvu nadzornih tijela sustava namire vrijednosnih papira kojima upravljaju središnji depozitoriji vrijednosnih papira, središnje banke koje izdaju najrelevantnije valute u kojima se provodi namira i središnje banke u čijim je knjigama namirena gotovinska strana transakcija ([34]). U tom pogledu, u uvodnoj izjavi 8. Uredbe o CSD-u navodi se da bi se Uredba trebala primjenjivati ne dovodeći u pitanje odgovornosti ESB-a i nacionalnih središnjih banaka u osiguranju učinkovitih i pouzdanih sustava poravnanja i platnih sustava unutar Unije i drugih zemalja. U uvodnoj izjavi 8. dalje se navodi da se Uredbom o CSD-u ne bi trebalo članovima ESSB-a priječiti pristup informacijama koje su važne za obavljanje njihovih dužnosti ([35]), uključujući nadzor središnjih depozitorija vrijednosnih papira i ostalih infrastruktura financijskog tržišta ([36]).

2.2.2 Osim toga, članovi ESSB-a često djeluju kao posrednici za namiru za gotovinsku stranu transakcija vrijednosnim papirima, a Eurosustav nudi usluge namire putem sustava T2S središnjim depozitorijima vrijednosnih papira. Nadzor Eurosustava nad sustavom T2S povezan je s njegovom ovlasti za osiguranje učinkovitog i pouzdanog sustava poravnanja i platnog sustava, dok nadležna i relevantna tijela središnjih depozitorija vrijednosnih papira nastoje osigurati njihovo nesmetano funkcioniranje, sigurnost i učinkovitost namire te pravilno funkcioniranje financijskih tržišta u svojim jurisdikcijama.

2.2.3 U skladu s Prijedlogom uredbe ([37]) središnje banke ESSB-a nisu uključene u razvoj tehničkih standarda u pogledu utvrđivanja rizika IKT-a. Slično tome, u skladu s Prijedlogom uredbe ([38]) odgovarajuća tijela nisu obaviještena ni o kakvim incidentima povezanim s IKT-om. Središnja banka ESSB-a trebala bi zadržati istu razinu uključenosti koja je trenutačno predviđena Uredbom o CSD-u, a relevantna tijela trebala bi biti obaviještena o incidentima povezanima s IKT-om. Eurosustav je odgovarajuće tijelo za sve središnje depozitorije vrijednosnih papira europodručja i za nekoliko drugih središnjih depozitorija vrijednosnih papira EU-a. Središnje banke ESSB-a trebale bi biti obaviještene o incidentima povezanima s IKT-om koji su relevantni za obavljanje njihovih dužnosti, uključujući nadzor središnjih depozitorija vrijednosnih papira i drugih infrastruktura financijskog tržišta. Rizici kojima su središnji depozitoriji vrijednosnih papira izloženi, uključujući rizike IKT-a, mogu ugroziti dobro funkcioniranje središnjih depozitorija vrijednosnih papira. Stoga su rizici IKT-a važni za odgovarajuća tijela, kojima bi trebalo pružiti potpun i detaljan pregled tih rizika kako bi ih se procijenilo i utjecalo na pristup središnjih depozitorija vrijednosnih papira upravljanju rizicima. Prijedlogom uredbe ne bi se trebali predvidjeti manje ograničavajući zahtjevi u pogledu rizika IKT-a u usporedbi s onima predviđenima Uredbom o CSD-u i postojećim povezanim regulatornim tehničkim standardima.

2.2.4 Osim toga, zakonodavna tijela Unije trebala bi pojasniti međudjelovanje Prijedloga uredbe ([39]) i regulatornih tehničkih standarda kojima se dopunjuje Uredba o CSD-u. Naročito, nije jasno treba li središnji depozitorij vrijednosnih papira biti izuzet od obveze posjedovanja vlastite sekundarne lokacije na kojoj njegova treća strana pružatelj IKT usluga održava takvu lokaciju ([40]). Ako bi središnji depozitorij vrijednosnih papira bio izuzet od obveze da održava sekundarnu lokaciju, nije jasno koju bi pravnu vrijednost imao taj zahtjev. Isto

([33]) Dostupno na mrežnim stranicama ESB-a www.ecb.europa.eu.

([34]) Vidi članak 12. Uredbe (EU) br. 909/2014.

([35]) Vidi također članak 13., članak 17. stavak 4. i članak 22. stavak 6. Uredbe (EU) br. 909/2014.

([36]) Vidi stavak 7.3 Mišljenja Europske središnje banke od 6. travnja 2017. o identifikaciji kritičnih infrastruktura za potrebe sigurnosti informacijske tehnologije (CON/2017/10); stavak 7.2 Mišljenja Europske središnje banke od 8. studenoga 2018. o određivanju ključnih usluga i operatora ključnih usluga za potrebe sigurnosti mrežnih i informacijskih sustava (CON/2018/47); stavak 3.5.2 Mišljenja Europske središnje banke od 2. svibnja 2019. o sigurnosti mrežnih i informacijskih sustava (CON/2019/17) i stavak 3.5.2 Mišljenja Europske središnje banke od 11. studenoga 2019. o sigurnosti mrežnih i informacijskih sustava (CON/2019/38).

([37]) Vidi članak 54. stavak 5. Prijedloga uredbe i članak 45. stavak 7. Uredbe (EU) br. 909/2014.

([38]) Vidi članak 54. stavak 4. Prijedloga uredbe i članak 45. stavak 6. Uredbe (EU) br. 909/2014.

([39]) Vidi članak 11. stavak 5. Prijedloga uredbe.

([40]) Vidi članak 78. stavak 3. Delegirane uredbe Komisije (EU) 2017/392 od 11. studenoga 2016. o dopuni Uredbe (EU) br. 909/2014 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda koji se odnose na zahtjeve za odobrenje, nadzor i objavu za središnje depozitorije vrijednosnih papira (SL L 65, 10.3.2017., str. 48.).

tako, Prijedlog uredbe ([41]) odnosi se na cilj u pogledu vremena oporavka i ciljeve u pogledu točke oporavka za svaku funkciju ([42]), dok se u odgovarajućem regulatornom tehničkom standardu razlikuju ključne funkcije ([43]) i ključne operacije ([44]) u odnosu na vrijeme oporavka utvrđeno za ključne operacije središnjih depozitorija vrijednosnih papira. Opravdano je da zakonodavna tijela Unije dodatno pojasne i promisle o međudjelovanju Prijedloga uredbe i regulatornih tehničkih standarda kojima se dopunjuje Uredba o CSD-u kako bi se izbjegao rizik postojanja proturječnih zahtjeva. Naposljetku, trebalo bi pojasniti da su izuzeća odobrena središnjim depozitorijima vrijednosnih papira kojima upravljaju određene osobe javnog prava u skladu s Uredbom o CSD-u ([45]) proširena Prijedlogom uredbe.

2.3 *Nadležnosti ESSB-a u području poravnanja vrijednosnih papira*

2.3.1 Središnjim bankama ESSB-a povjerene su nadzorne ovlasti u odnosu na središnje druge ugovorne strane. U tom pogledu, nacionalne središnje banke Eurosustava često surađuju s odgovarajućim nacionalnim nadležnim tijelima u nadzornim i supervizorskim funkcijama središnjih drugih ugovornih strana i sudjeluju u odnosnom kolegiju središnjih drugih ugovornih strana osnovanom na temelju Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća ([46]) (dalje u tekstu „EMIR"). Odgovarajući članovi Eurosustava ([47]) sudjeluju u kolegijima EMIR-a u svojoj nadzornoj funkciji i predstavljaju Eurosustav kao središnju banku izdanja središnjih drugih ugovornih strana gdje je euro jedna od najvažnijih valuta za financijske instrumente čije se poravnanje obavlja (i za izvanteritorijalne središnje druge ugovorne strane koje poravnavaju znatan udio financijskih instrumenata u euru). ESB je središnja banka izdanja središnjih drugih ugovornih strana izvan europodručja.

2.3.2 U skladu s Prijedlogom uredbe ([48]) središnje banke ESSB-a nisu uključene u pripremu tehničkih standarda u pogledu utvrđivanja rizika IKT-a. Osim toga, u Prijedlogu uredbe ([49]) ne upućuje se ni na cilj u pogledu vremena oporavka ni na zahtjeve u odnosu na cilj u pogledu točke oporavka u skladu s EMIR-om ([50]). Predloženim regulatornim ustrojem ne bi se trebali predvidjeti manje ograničavajući zahtjevi u pogledu rizika IKT-a od onih koji trenutačno postoje. Stoga je ključno odrediti jasno vrijeme i ciljeve u pogledu razdoblja oporavka kako bi se uspostavio čvrst okvir za upravljanje kontinuitetom poslovanja. Održavanje posebnih rokova i ciljeva u pogledu razdoblja oporavka također je dio Načela CPMI-IOSCO-a za infrastrukture financijskih tržišta ([51]). Trebalo bi zadržati postojeću odredbu u okviru EMIR-a te bi Prijedlog uredbe trebalo na odgovarajući način prilagoditi. Središnje banke ESSB-a trebale bi sudjelovati u pripremi sekundarnog zakonodavstva, kao i u daljnjem pojašnjenju i promišljanju zakonodavnih tijela Unije o međudjelovanju Prijedloga uredbe i regulatornih tehničkih standarda koji je dopunjuju kako bi se izbjegao rizik od proturječnih ili preklapajućih zahtjeva.

3. **Posebna opažanja o aspektima bonitetnog nadzora**

3.1 Uredbom Vijeća (EU) br. 1024/2013 ([52]) (dalje u tekstu „Uredba o SSM-u") ESB-u se dodjeljuju posebne zadaće u vezi s bonitetnim nadzorom kreditnih institucija u europodručju te ESB postaje odgovoran za učinkovito i dosljedno funkcioniranje jedinstvenog nadzornog mehanizma (SSM), u okviru kojeg se posebne nadzorne odgovornosti raspodjeljuju između ESB-a i nacionalnih nadležnih tijela sudionika. Posebno, ESB obavlja zadaću izdavanja odobrenja za rad i oduzimanja odobrenja za rad svim kreditnim institucijama. ESB također ima zadaću, među ostalim, osigurati usklađenost s relevantnim zakonima Unije kojima se propisuju bonitetni zahtjevi za kreditne institucije, uključujući zahtjev za uspostavu pouzdanih sustava upravljanja, kao što su pouzdani postupci upravljanja rizikom i mehanizmi unutarnjih kontrola ([53]). U tu svrhu ESB-u su dodijeljene sve nadzorne ovlasti da intervenira u djelatnosti kreditnih institucija koje su potrebne za izvršavanje njegovih funkcija. Stoga su ESB i odgovarajuća nacionalna nadležna tijela, nadležna tijela koja izvršavaju određene ovlasti bonitetnog nadzora u

([41]) Vidi članak 11. stavak 6. Prijedloga uredbe.
([42]) Vidi članak 3. stavak 17. Prijedloga uredbe.
([43]) Vidi članak 76. stavak 2. točke (d) i (e) Delegirane uredbe Komisije (EU) 2017/392.
([44]) Vidi članak 78. stavke 2. i 3. Delegirane uredbe Komisije (EU) 2017/392.
([45]) Vidi članak 1. stavak 4. Uredbe (EU) br. 909/2014.
([46]) Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27.7.2012., str. 1.).
([47]) Vidi članak 18. stavak 2. točke (g) i (h) EMIR-a.
([48]) Vidi članak 53. stavak 2. točku (b) i stavak 3. Prijedloga uredbe te članak 34. stavak 3. EMIR-a.
([49]) Vidi članak 53. stavak 2. točku (a) Prijedloga uredbe.
([50]) Vidi članak 34. EMIR-a.
([51]) VIDI CPMI-IOSCO Načela za infrastrukture financijskih tržišta dostupna na mrežnim stranicama Banke za međunarodne namire: www.bis.org.
([52]) Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29.10.2013., str. 63.).
([53]) Vidi članak 4. stavak 1. točku (e) i članak 6. stavak 4. Uredbe (EU) br. 1024/2013.

skladu s Uredbom 2013/575/EU Europskog parlamenta i Vijeća ([54]) (dalje u tekstu: „Uredba o kapitalnim zahtjevima") i Direktivom 2013/36/EU Europskog parlamenta i Vijeća ([55]) (dalje u tekstu „Direktiva o kapitalnim zahtjevima").

3.2 U Prijedlogu uredbe navodi se da bi trebalo dodatno razviti jedinstvena pravila i sustav nadzora kako bi se obuhvatili digitalna operativna otpornost i sigurnost IKT-a proširenjem ovlasti financijskih nadzornih tijela zaduženih za praćenje i zaštitu financijske stabilnosti i cjelovitosti tržišta ([56]). Cilj je uspostaviti sveobuhvatan okvir za IKT ili operativni rizik usklađivanjem ključnih zahtjeva za digitalnu operativnu otpornost za sve financijske subjekte ([57]). Konkretno, cilj je Prijedloga uredbe konsolidirati i unaprijediti zahtjeve u pogledu rizika IKT-a koji su dosad zasebno obrađeni u različitim zakonodavnim aktima ([58]).

3.3 Zahtjevi povezani s rizikom IKT-a za financijski sektor trenutačno su raspoređeni na niz pravnih akata Unije, uključujući Direktivu o kapitalnim zahtjevima, i neobvezujuće pravne instrumente (kao što su smjernice EBA-e) te su raznoliki i povremeno nepotpuni. U nekim je slučajevima rizik IKT-a samo implicitno reguliran kao dio operativnog rizika, dok se u drugima uopće ne regulira. To bi trebalo ispraviti usklađivanjem Prijedloga uredbe s tim aktima. U tu svrhu Prijedlogom direktive o izmjeni predlaže se niz izmjena koje se čine potrebnima kako bi se postigla pravna jasnoća i dosljednost u odnosu na primjenu različitih zahtjeva za digitalnu operativnu otpornost. Međutim, izmjene Direktive o kapitalnim zahtjevima koje su trenutačno predložene Prijedlogom direktive o izmjeni ([59]) odnose se samo na odredbe o planovima za nepredviđene situacije i planove kontinuiteta poslovanja ([60]), s obzirom na to da, navodno, implicitno služe kao osnova za reguliranje pitanja upravljanja rizikom IKT-a.

3.4 Nadalje, Prijedlogom uredbe ([61]) predviđa se da financijski subjekti, uključujući kreditne institucije, imaju uspostavljene okvire za unutarnje upravljanje i kontrolu kojima se osigurava učinkovito i razborito upravljanje svim rizicima IKT-a. Prijedlogom uredbe ([62]) predviđa se primjena u njoj utvrđenih zahtjeva na pojedinačnoj i konsolidiranoj razini, ali bez dovoljne usklađenosti s navedenim sektorskim zakonodavstvom na koje se odnosi. Naposljetku, u skladu s Prijedlogom uredbe ([63]), predviđeno je da, ne dovodeći u pitanje odredbe o nadzornom okviru za treće strane pružatelje ključnih IKT usluga navedene u Prijedlogu uredbe ([64]), ispunjavanje obveza utvrđenih u Prijedlogu uredbe osigurava, za kreditne institucije, nadležno tijelo imenovano u skladu s člankom 4. Direktive o kapitalnim zahtjevima, ne dovodeći u pitanje posebne zadaće dodijeljene ESB-u Uredbom o SSM-u.

3.5 S obzirom na prethodno navedeno, ESB razumije da se, u odnosu na kreditne institucije s iznimkom odredbi Prijedloga uredbe koje se odnose na nadzorni okvir za treće osobe pružatelje ključnih usluga IKT-a, ([65]), Prijedlogom uredbe namjerava uspostaviti bonitetni okvir unutarnjeg upravljanja za upravljanje rizikom IKT-a koji će biti uključen u opći okvir unutarnjeg upravljanja u okviru Direktive o kapitalnim zahtjevima. Nadalje, s obzirom na bonitetnu prirodu predloženog okvira, nadležna tijela odgovorna za nadzor usklađenosti s obvezama utvrđenima u predloženom okviru, uključujući ESB, bit će tijela odgovorna za nadzor banaka u skladu s Uredbom o SSM-u.

([54]) Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

([55]) Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

([56]) Vidi uvodnu izjavu 8. Prijedloga uredbe.

([57]) Vidi uvodnu izjavu 11. Prijedloga uredbe.

([58]) Vidi uvodnu izjavu 12. Prijedloga uredbe.

([59]) Vidi uvodne izjave 4. i 5. Prijedloga direktive o izmjeni.

([60]) Vidi članak 85. Direktive o kapitalnim zahtjevima.

([61]) Vidi članak 4. stavak 1. Prijedloga uredbe.

([62]) Vidi članak 25. stavak 3. točku 4. Prijedloga uredbe.

([63]) Vidi članak 41. Prijedloga uredbe.

([64]) Vidi poglavlje V. odjeljak II. Prijedloga uredbe.

([65]) Vidi poglavlje V. odjeljak II. Prijedloga uredbe.

3.6 Zakonodavna tijela Unije stoga će možda htjeti uzeti u obzir sljedeće prijedloge za povećanje jasnoće i koordinacije između Prijedloga uredbe i Direktive o kapitalnim zahtjevima. Prvo, zahtjevi iz Prijedloga uredbe mogu se izričito smatrati bonitetnima, kao što je to učinjeno, među ostalim, u Uredbi o CSD-u ([66]). Drugo, uvodne izjave Prijedloga direktive o izmjeni ([67]), mogle bi proširiti njihov tekst s obzirom na to da zahtjevi iz Prijedloga uredbe nadilaze jedinu fazu nacrta za izvanredne situacije i kontinuitet poslovanja. Općenito, mjere upravljanja rizikom IKT-a obuhvaćene su općenitijim područjem primjene pouzdanih pravila upravljanja u skladu s člankom 74. Direktive o kapitalnim zahtjevima ([68]). Treće, Prijedlog uredbe ([69]) trebalo bi izmijeniti kako bi se u uvodnim izjavama podsjetilo na nadležnost ESB-a za bonitetni nadzor kreditnih institucija u skladu s Ugovorom i Uredbom o SSM-u. Četvrto, upućivanje na primjenu u njoj predviđenih zahtjeva na pojedinačnoj i konsolidiranoj razini ([70]) trebalo bi revidirati jer potkonsolidirane i konsolidirane razine nisu definirane u Prijedlogu uredbe, a određene vrste posrednika ne podliježu konsolidiranom nadzoru u skladu s relevantnim zakonodavstvom (npr. institucije za platni promet). Nadalje, razina primjene zahtjeva u okviru Prijedloga uredbe trebala bi proizlaziti isključivo iz zakonodavstva koje se primjenjuje na svaku vrstu financijskog subjekta. U slučaju kreditnih institucija predviđena je jasna veza između Direktive o kapitalnim zahtjevima i Prijedloga uredbe te bi se stoga zahtjevi iz Prijedloga uredbe automatski primjenjivali na pojedinačnoj, potkonsolidiranoj ili konsolidiranoj razini ([71]), ovisno o slučaju. Naposljetku, zakonodavna tijela Unije mogla bi razmotriti uvođenje prijelaznog režima za upravljanje razdobljem od stupanja na snagu Prijedloga uredbe do stupanja na snagu regulatornih tehničkih standarda predviđenih Prijedlogom uredbe, s obzirom na to da neki posrednici, uključujući kreditne institucije, već podliježu pravilima o rizicima IKT-a koja se primjenjuju na određene sektore i koji su detaljniji od općih odredaba Prijedloga uredbe.

3.7 ESB-u je na temelju Uredbe o SSM-u povjerena zadaća osiguravanja usklađenosti kreditnih institucija sa zahtjevima prava Unije kojima se od kreditnih institucija zahtijeva da imaju uspostavljene pouzdane postupke upravljanja rizicima i mehanizme unutarnje kontrole ([72]). To znači da ESB mora osigurati da kreditne institucije provode politike i procese za vrednovanje izloženosti operativnom riziku i upravljanje njome, uključujući rizik modela, i za pokriće događaja male učestalosti s velikim gubicima. Od kreditnih institucija zahtijeva se da odrede što predstavlja operativni rizik za potrebe ovih politika i postupaka ([73]).

3.8 Upravno vijeće Europske središnje banke (ESB) donijelo je u srpnju 2017. Okvir za izvješćivanje o kiberincidentima SSM-a (dalje u tekstu „Okvir”) na temelju nacrta prijedloga Nadzornog odbora u skladu s člankom 26. stavkom 8. i člankom 6. stavkom 2. Uredbe o SSM-u te člankom 21. stavkom 1. Uredbe (EU) br. 468/2014 Europske središnje banke (ESB/2014/17) ([74]). Okvir se sastoji od obvezujućeg zahtjeva (pojedinačne odluke upućene kreditnim institucijama) za informacije i/ili izvješćivanje na temelju članka 10. Uredbe o SSM-u ([75]). Neke zemlje već su uspostavile postupak izvješćivanja o incidentima kojim se od kreditnih institucija zahtijeva da prijave sve važne kiberincidente svojim nacionalnim nadležnim tijelima. U tim će zemljama značajne kreditne institucije i dalje izvješćivati nacionalna nadležna tijela o incidentima, koja će ih zatim bez nepotrebnog odlaganja proslijediti ESB-u

([66]) Vidi naslov poglavlja II. odjeljka 4. „Bonitetni zahtjevi” Uredbe o CSD-u.

([67]) Vidi uvodnu izjavu 4. Prijedloga direktive o izmjeni.

([68]) Članak 85. Direktive 2013/36/EU je samo specifikacija. U tom pogledu vidi i stranice 4., 11. i 37. Smjernica Europskog nadzornog tijela za bankarstvo o upravljanju rizicima informacijske i komunikacijske tehnologije i sigurnosnim rizicima od 29. studenoga 2019. (dalje u tekstu „Smjernice EBA-e”), u kojima se opća pravna osnova izričito nalazi u članku 74. Direktive 2013/36/EU.

([69]) Vidi članak 41. stavak 1. Prijedloga uredbe.

([70]) Vidi članak 25. stavke 3. i 4. Prijedloga uredbe.

([71]) Vidi također članak 109. Direktive o kapitalnim zahtjevima.

([72]) Vidi članak 4. stavak 1. točku (e) Uredbe o SSM-u.

([73]) Vidi članak 85. Direktive o kapitalnim zahtjevima.

([74]) Uredba (EU) br. 468/2014 Europske središnje banke od 16. travnja 2014. o uspostavljanju okvira za suradnju unutar jedinstvenog nadzornog mehanizma između Europske središnje banke i nacionalnih nadležnih tijela te s nacionalnim imenovanim tijelima (Okvirna uredba o SSM-u) (ESB/2014/17) (SL L 141, 14.5.2014., str. 1).

([75]) Konkretno, kiberincident (utvrđena moguća povreda informacijske sigurnosti, bilo zlonamjerno ili slučajno) mora se prijaviti ESB-u ako je ispunjen barem jedan od sljedećih uvjeta: (1) postoji mogući financijski učinak od 5 milijuna eura ili 0,1 % redovnog osnovnog kapitala, (2) incident je javno objavljen ili je prouzročio reputacijsku štetu, (3) incident je eskaliran do CIO izvan redovnog izvješćivanja, (4) banka je obavijestila o incidentu CERT/CSIRT sigurnosnu agenciju ili policiju (5) oporavak od katastrofe ili postupak kontinuiteta poslovanja su inicirani ili su podneseni zahtjevi za osiguranje kibersigurnosti (6) došlo je do povrede pravnih ili regulatornih zahtjeva ili (7) banka primjenjuje interne kriterije i stručnu prosudbu (uključujući mogući sistemski učinak) i odlučuje o tome obavijestiti ESB.

u ime nadziranih subjekata. Stoga se gore navedene odluke upućuju i tim nacionalnim nadležnim tijelima da te informacije proslijede ESB-u na temelju Okvira. ESB podupire nastojanja zakonodavnih tijela Unije da promiču usklađivanje i racionalizaciju, među ostalim, u pogledu skupa pravila i obveza primjenjivih na kreditne institucije u pogledu izvješćivanja o incidentima. S obzirom na to, ESB je spreman prema potrebi izmijeniti (i potencijalno staviti izvan snage) Okvir, s obzirom na moguće donošenje Prijedloga uredbe.

4. **Posebna opažanja o upravljanju rizikom IKT-a, izvješćivanju o incidentima, testiranju operativne otpornosti i riziku treće strane u području IKT-a**

4.1 *Upravljanje rizikom IKT-a*

4.1.1 ESB pozdravlja činjenicu da je Prijedlogom uredbe uveden pouzdan i sveobuhvatan okvir za upravljanje rizikom IKT-a koji obuhvaća Smjernice CPMI-IOSCO-a o kiberotpornosti i koji je usko usklađen s najboljim praksama, uključujući očekivanja Eurosustava o nadzoru u vezi s kiberotpornošću za infrastrukture financijskog tržišta.

4.1.2 ESB podržava ideju da bi financijski subjekti trebali provoditi procjenu rizika nakon svake „značajne promjene" u infrastrukturi mrežnih i informacijskih sustava ([76]). Međutim, Prijedlog uredbe ne sadrži definiciju „značajne promjene", čime se stvara nepoželjan prostor za različita tumačenja financijskih subjekata koja bi u konačnici mogla ugroziti ciljeve Prijedloga uredbe u vezi s usklađivanjem. Radi pravne sigurnosti zakonodavna tijela Unije možda bi željela razmotriti uvođenje definicije „značajne promjene" u Prijedlog uredbe.

4.1.3 ESB općenito podržava ideju da financijski subjekti koji nisu mikropoduzeća nadležnim tijelima prijavljuju odgovarajuće troškove i gubitke uzrokovane poremećajima IKT-a i incidente povezane s IKT-om ([77]). Međutim, kako bi se osigurala sveobuhvatna učinkovitost sustava i izbjegla mogućnost preopterećenja nadležnih tijela i financijskih subjekata s prevelikim brojem izvješća, moglo bi biti korisno da zakonodavna tijela Unije istraže uvođenje odgovarajućih pragova, po mogućnosti kvantitativne prirode.

4.1.4 ESB priznaje mogućnost da financijski subjekti prenose poduzećima unutar grupe ili vanjskim poduzećima zadaće provjere usklađenosti sa zahtjevima za upravljanje rizikom IKT-a, uz odobrenje nadležnih tijela ([78]). Istodobno je važno da zakonodavna tijela Unije pojasne kako bi se odobrenje nadležnih tijela dalo u slučajevima u kojima financijski subjekt podliježe većem broju nadležnih tijela. Do toga može doći ako je financijski subjekt kreditna institucija, pružatelj usluga kriptoimovine i/ili pružatelj platnih usluga. Naposljetku, u odnosu na utvrđivanje i klasifikaciju koju provode financijski subjekti na temelju Prijedloga uredbe ([79]), ESB bi za potrebe klasifikacije imovine smatrao razboritim da se Prijedlogom uredbe od financijskih subjekata zahtijeva da uzmu u obzir je li takva imovina ključna (tj. podržava li ključne funkcije).

4.2 *Izvješćivanje o incidentima*

4.2.1 ESB pozdravlja napore navedene u Prijedlogu uredbe za usklađivanje okruženja izvješćivanja o incidentima u području IKT-a u Uniji i rad na centraliziranom izvješćivanju o značajnim IKT incidentima ([80]). Uvođenjem usklađenog okvira za izvješćivanje odgovarajućih nadležnih tijela o značajnim IKT incidentima ([81]) u načelu bi se pojednostavnio i uskladio teret izvješćivanja financijskih subjekata, uključujući kreditne institucije. Nadležna tijela imala bi koristi od šireg raspona obuhvaćenih incidenata, koji nadilaze kibernetske incidente koji su trenutačno obuhvaćeni postojećim okvirima ([82]). Buduće donošenje Prijedloga uredbe zahtijevalo bi preispitivanje i moguće stavljanje izvan snage postojećih okvira, uključujući Okvir za izvješćivanje o kiberincidentima u SSM-u. Međutim, kako bi se postiglo istinsko pojednostavnjenje i potpuna usklađenost u svim okvirima, ključno je osigurati potpunu usklađenost područja primjene odredbi o izvješćivanju o incidentima iz Prijedloga uredbe, uključujući sve relevantne definicije, pragove i parametre izvješćivanja. Posebno, od iznimne je važnosti osigurati usklađenost

([76]) Vidi članak 7. stavak 3. Prijedloga uredbe.
([77]) Vidi članak 10. stavak 9. Prijedloga uredbe.
([78]) Vidi članak 5. stavak 10. Prijedloga uredbe.
([79]) Vidi članak 7. Prijedloga uredbe.
([80]) Vidi članak 19. Prijedloga uredbe.
([81]) Vidi članak 3. stavak 7. i članke 17. i 18. Prijedloga uredbe.
([82]) Vidi primjerice Okvir.

između, s jedne strane, Prijedloga uredbe i, s druge strane, Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća ([83]) (dalje u tekstu „PSD2") i EBA-inih Smjernica o izvješćivanju o značajnim incidentima (dalje u tekstu „Smjernice EBA-e"). Prijedlog direktive o izmjeni ([84]) sadrži izmjene direktive PSD2 u vezi s razgraničenjem izvješćivanja o incidentima između Prijedloga uredbe i direktive PSD2, što bi uglavnom utjecalo na pružatelje platnih usluga, koji bi također mogli imati odobrenje za rad kao kreditne institucije, kao i na nadležna tijela. Postupak obavješćivanja o incidentima nije dovoljno jasan te postoji mogućnost preklapanja između nekih incidenata koje je potrebno prijaviti u skladu s Prijedlogom uredbe i Smjernicama EBA-e.

4.2.2 Postupcima za obavješćivanje o značajnim incidentima u skladu s Prijedlogom uredbe ([85]), Direktivom PSD2 i odgovarajućim Smjernicama EBA-e od pružatelja platnih usluga zahtijevalo bi se da nakon klasificiranja incidenta podnesu izvješće o incidentima svojem nadležnom tijelu. Zapravo, početna izvješća ne obuhvaćaju bit, uzrok ili funkcionalno područje na koje incident utječe, a pružatelji platnih usluga mogu napraviti takve razlike tek u kasnijoj fazi kada postanu dostupne detaljnije informacije o incidentu. Kao rezultat toga, početna izvješća o incidentima mogla bi se podnositi i u skladu s Prijedlogom uredbe i Smjernicama EBA-e, ili pružatelji platnih usluga mogu odlučiti o jedinstvenom okviru za izvješćivanje i naknadno ispraviti svoje podneske. Ista nesigurnost (primjerice u pogledu temeljnog uzroka bilo kojeg incidenta) može se odraziti i u međuizvješćima i završnim izvješćima. Time bi se ponovno povećala mogućnost za usporedno podnošenje izvješća nadležnim tijelima u skladu s Prijedlogom uredbe i Direktivom PSD2.

4.2.3 Neki incidenti koji se mogu kategorizirati kao incidenti povezani s IKT-om mogu utjecati i na druga područja te bi zbog toga morali biti prijavljeni u skladu sa Smjernicama EBA-e. To može biti slučaj ako incident ima utjecaj iz perspektive IKT-a, ali istodobno ima utjecaj na izravno pružanje platnih usluga i/ili druga funkcionalna područja ili kanale koji nisu povezani s IKT-om. Osim toga, moglo bi biti slučajeva u kojima nije moguće razlikovati operativne incidente i incidente povezane s IKT-om. Nadalje, u slučaju kada je isti financijski subjekt značajna kreditna institucija i pružatelj platnih usluga, u skladu s Prijedlogom uredbe isti bi subjekt morao dvaput prijaviti incident povezan s IKT-om, zbog toga što podliježe dvama nadležnim tijelima. S obzirom na prethodno navedeno, u Prijedlogu uredbe trebalo bi jasnije formulirati kako bi međudjelovanje Direktive PSD2 i Smjernica EBA-e trebalo funkcionirati u praksi. Što je još važnije, bilo bi važno, radi usklađivanja i pojednostavnjenja obveza izvješćivanja, da zakonodavna tijela Unije razmotre preostala pitanja dvostrukog izvješćivanja te da se razjasni hoće li Prijedlog uredbe s jedne strane te Direktiva PSD2 i Smjernice EBA-e s druge strane istodobno postojati ili bi trebao postojati jedinstveni skup zahtjeva za izvješćivanje o incidentima.

4.2.4. Prijedlogom uredbe uvodi se zahtjev prema kojem nadležna tijela ([86]) nakon primitka izvješća moraju potvrditi primitak obavijesti i što je prije moguće pružiti sve potrebne povratne informacije ili smjernice financijskom subjektu, posebno kako bi se raspravile korektivne mjere na razini subjekta ili načini minimiziranja nepovoljnih učinaka u svim sektorima. To bi značilo da bi nadležna tijela trebala aktivno doprinositi upravljanju incidentima i njihovu saniranju, istodobno procjenjujući odgovor nadziranog subjekta na kritične incidente. ESB naglašava da bi odgovornost za sanaciju i posljedice incidenta te vlasništvo nad njim trebali ostati isključivo i jasno na dotičnom financijskom subjektu. ESB stoga predlaže da se povratne informacije i smjernice ograniče samo na bonitetne povratne informacije i smjernice na visokoj razini. Ako bi povratne informacije bile šire, to bi zahtijevalo specijalizirane stručnjake sa značajnim tehničkim znanjem koje obično nije dostupno u bazi talenata dostupnoj bonitetnim tijelima.

4.3 *Testiranje digitalne operativne otpornosti*

4.3.1 ESB pozdravlja zahtjeve utvrđene u Prijedlogu uredbe ([87]) o testiranju digitalne operativne otpornosti u financijskim subjektima i potrebu da svaka institucija ima vlastiti program testiranja. U Prijedlogu uredbe ([88]) opisuju se različite vrste testiranja kao pokazatelj za financijske subjekte. Vrste testova nisu potpuno jasne, a europska nadzorna tijela, nadležna tijela ili financijski subjekti mogu tumačiti neke testove, kao što su testovi kompatibilnosti, upitnici ili

([83]) Direktiva (EU) 2015/2366 Europskog parlamente i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35.).

([84]) Vidi članak 7. stavak 9. Prijedloga direktive o izmjeni.

([85]) Vidi članak 17. stavak 3. Prijedloga uredbe.

([86]) Vidi članak 20. Prijedloga uredbe.

([87]) Vidi članke 21. i 22. Prijedloga uredbe.

([88]) Vidi članak 22. stavak 1. Prijedloga uredbe.

testovi koji se temelje na scenarijima. Osim toga, ne postoje ni smjernice o učestalosti svakog testiranja. Mogući pristup mogao bi biti da se Prijedlogom uredbe utvrde generički zahtjevi za testiranje, s preciznijim opisom vrsta testiranja koje se utvrđuju regulatornim i provedbenim tehničkim standardima.

4.3.2 Penetracijska testiranja vođena prijetnjama (TLPT) moćan su alat za testiranje sigurnosne obrane i pripravnosti. ESB stoga potiče financijske subjekte na TLPT. Ovim se alatom ne ispituju samo tehničke mjere, već i osoblje i procesi. Rezultati tih testiranja mogu znatno povećati razinu svijesti višeg rukovodstva o sigurnosti unutar subjekata koji se testiraju. Europski okvir za etičko hakiranje koje se zasniva na obavještajnim podacima o prijetnjama (TIBER-EU) ([89]) i drugi alati TLPT-a koji su već dostupni izvan Unije primarni su instrumenti kojima subjekti sami procjenjuju, testiraju, vježbaju i poboljšavaju svoj položaj i obranu u pogledu kiberotpornosti.

4.3.3 U većini država članica u kojima je proveden TIBER-EU, nadzorna tijela nemaju aktivnu ulogu u provedbi lokaliziranog programa TIBER-XX, a kibernetički tim TIBER-a (TCT) smješten je u gotovo svim slučajevima neovisno o tim funkcijama. Stoga bi se napredna testiranja u okviru Prijedloga uredbe ([90]), s pomoću TLPT-a, trebala provoditi kao alat za jačanje financijskog ekosustava i jačanje financijske stabilnosti, a ne samo kao alat za nadzor. Osim toga, nema potrebe za razvojem novog naprednog okvira za testiranje kiberotpornosti jer su države članice već u velikoj mjeri usvojile TIBER-EU, jedini takav okvir u EU-u.

4.3.4 Zahtjevi za provoditelje testiranja ne bi trebali biti sadržani u glavnom dijelu Prijedloga uredbe jer se sektor povezan s TLPT-om i dalje razvija, a inovacije mogu biti otežane određivanjem posebnih zahtjeva. S obzirom na navedeno, ESB smatra da, kako bi se osigurao visok stupanj neovisnosti pri provođenju testiranja, financijski subjekti ne bi trebali zapošljavati niti sklopiti ugovor s provoditeljima testiranja koji su zaposleni ili ugovorno angažirani od strane financijskih subjekata u svojoj grupi ili koji su na neki drugi način u vlasništvu i/ili pod kontrolom financijskih subjekata koje treba testirati.

4.3.5 Kako bi se smanjio rizik od fragmentacije i osigurala usklađenost, Prijedlogom uredbe trebalo bi propisati jedan okvir TLPT-a koji se primjenjuje na financijski sektor u cijeloj Uniji. Fragmentacija može dovesti do povećanja troškova te tehničkih, operativnih i financijskih zahtjeva, kako za nadležna tijela tako i za financijske institucije. Ti povećani troškovi i zahtjevi u konačnici mogu negativno utjecati na uzajamno priznavanje testiranja. Taj nedostatak usklađenosti i problemi povezani s uzajamnim priznavanjem koji iz toga proizlaze posebno su važni za financijske subjekte koji mogu imati višestruke licencije i/ili poslovati u više jurisdikcija diljem Unije. Regulatorni i provedbeni tehnički standardi, koji će se izrađivati za TLPT u skladu s Prijedlogom uredbe, trebali bi biti u skladu s TIBER-EU-om. Nadalje, ESB pozdravlja mogućnost sudjelovanja u pripremi tih regulatornih i provedbenih tehničkih standarda u suradnji s europskim nadzornim tijelima.

4.3.6 Aktivna uključenost nadležnih tijela u testiranja mogla bi dovesti do mogućeg sukoba interesa s drugom funkcijom koju obavljaju, tj. procjenom okvira za testiranje financijskog subjekta. U tom kontekstu ESB predlaže da se iz Prijedloga uredbe uklone sve obveze nadležnih tijela u pogledu validacije dokumenata i izdavanja potvrde za test TLPT.

4.4 IKT rizik treće strane

4.4.1 ESB pozdravlja uvođenje sveobuhvatnog skupa ključnih načela i pouzdanog nadzornog okvira za utvrđivanje rizika IKT-a koji proizlaze iz trećih pružatelja usluga IKT-a i upravljanje njime, bez obzira na to pripadaju li istoj grupi financijskih subjekata. Međutim, kako bi se postigla učinkovita identifikacija rizika IKT-a i upravljanje njime, važno je točno utvrditi i klasificirati, među ostalim, treće strane pružatelje ključnih usluga IKT-a. U tom pogledu, iako je uvođenje delegiranih akata ([91]) kojima će se dopuniti kriteriji koji se upotrebljavaju za potrebe klasifikacije ([92]) dobrodošlo, s ESB-om bi se trebalo savjetovati prije donošenja takvih delegiranih akata.

([89]) Dostupno na mrežnim stranicama ESB-a, www.ecb.europa.eu.
([90]) Članci 23. i 24. Prijedloga uredbe.
([91]) Vidi članak 28. stavak 3. Prijedloga uredbe.
([92]) Vidi članak 28. stavak 2. Prijedloga uredbe.

4.4.2 Što se tiče strukture nadzornog okvira ([93]), potrebno je dodatno pojasniti ulogu koju treba preuzeti Zajednički odbor. Istodobno, ESB pozdravlja svoje uključivanje u Nadzorni forum kao promatrača jer će ta uloga omogućiti ESB-u jednak pristup dokumentaciji i informacijama kakav imaju i članovi s pravom glasa ([94]). ESB bi želio skrenuti pozornost zakonodavnih tijela Unije na činjenicu da bi ESB, u svojoj ulozi promatrača, pridonosio radu Nadzornog foruma u svojstvu središnje banke izdanja, odgovorne za nadzor tržišne infrastrukture i bonitetnog nadzornog tijela nad kreditnim institucijama. Nadalje, ESB napominje da bi ESB, osim što je promatrač u Nadzornom forumu, također bio dio zajedničkog tima za provjere kao nadležno tijelo. Zakonodavna tijela Unije mogla bi u tom pogledu dodatno razmotriti sastav zajedničkih timova za provjere ([95]) kako bi se osiguralo odgovarajuće intenzivno sudjelovanje relevantnih nadležnih tijela. Isto tako, ESB smatra da bi trebalo povećati najveći broj sudionika u zajedničkim timovima za provjere, uzimajući u obzir kritičnost, složenost i opseg usluga treće strane u području IKT-a.

4.4.3 ESB napominje da u skladu s Prijedlogom uredbe, glavno nadzorno tijelo može spriječiti treće strane pružatelje ključnih usluga IKT-a da sklapaju daljnje sporazume o podugovaranju u kojima je i. predviđeni podugovaratelj treća strana u području IKT-a ili podizvođač za IKT sa sjedištem u trećoj zemlji i ii. ako se podugovaranje odnosi na ključnu ili važnu funkciju financijskog subjekta. ESB želi naglasiti da te ovlasti može izvršavati samo glavno nadzorno tijelo u kontekstu aranžmana o podugovaranju kada treća strana pružatelj ključnih usluga IKT-a podugovara ključnu ili važnu funkciju zasebnom pravnom subjektu sa sjedištem u trećoj zemlji. ESB razumije da glavno nadzorno tijelo ne bi moglo izvršavati usporedive ovlasti kako bi spriječio treću stranu pružatelja ključnih usluga IKT-a da eksternalizira ključne ili važne funkcije financijskog subjekta u objekte tog pružatelja usluga koji se nalaze u trećoj zemlji. Primjerice, moglo bi se dogoditi da se, s operativnog stajališta, ključni podaci i/ili informacije mogu pohraniti ili obraditi u objektima smještenima izvan Europskog gospodarskog prostora (EGP). U tom slučaju ovlasti vodećeg nadzornog tijela ne smiju na odgovarajući način ovlastiti nadležna tijela za pristup svim informacijama, poslovnim prostorijama, infrastrukturi i osoblju koji su važni za obavljanje svih ključnih ili važnih funkcija financijskog subjekta. Kako bi se osiguralo da nadležna tijela mogu neometano obavljati svoje zadaće, ESB predlaže da bi glavnom nadzornom tijelu trebalo dodijeliti ovlast da ograniči uporabu objekata smještenih izvan EGP-a od strane trećih osoba pružatelja ključnih usluga IKT-a. Ta bi se ovlast mogla izvršavati u onim posebnim slučajevima u kojima nisu uspostavljeni administrativni dogovori s relevantnim tijelima trećih zemalja, kako je predviđeno Prijedlogom uredbe ([96]), ili ako predstavnici trećih strana pružatelja ključnih usluga IKT-a ne daju dovoljna jamstva u okviru relevantne treće zemlje u pogledu pristupa informacijama, poslovnim prostorijama, infrastrukturi i osoblju koji su potrebni za provođenje nadzornih ili supervizorskih zadaća.

4.4.4 Naposljetku, zahtijevanje od nadležnih tijela da postupaju u skladu s preporukama vodećeg nadzornog tijela ([97]) može se pokazati neučinkovitim jer nadležna tijela možda nemaju cjelovit pristup rizicima koje stvara svaka treća strana pružatelj ključnih usluga IKT-a. Osim toga, od nadležnih tijela može se zahtijevati da poduzmu mjere protiv svojih nadziranih financijskih subjekata ako treće strane koje su pružatelji ključnih usluga ne primjenjuju preporuke. U skladu s Prijedlogom uredbe ([98]) nadležna tijela mogu zahtijevati od svojih nadziranih financijskih subjekata da privremeno obustave ključne usluge koje pružaju treće strane ili da raskinu neispunjene ugovore s trećim stranama pružateljima ključnih usluga. Predviđeni postupak praćenja teško je pretočiti u konkretne mjere. Konkretno, nije jasno hoće li nadzirani financijski subjekt biti u mogućnosti privremeno obustaviti ili raskinuti ugovor s trećom stranom pružateljem ključnih usluga. Razlog tomu je činjenica da bi treća strana pružatelj ključnih usluga IKT-a mogao biti značajan pružatelj za tog financijskog subjekta ili zbog troškova i štete, ugovornih ili drugih, koje bi financijski subjekt mogao pretrpjeti zbog takve privremene obustave ili raskida. Nadalje, tim se pristupom ne podupire konvergencija nadzora jer nadležna tijela mogu različito tumačiti istu preporuku. To bi u konačnici moglo ugroziti predviđeno usklađivanje i dosljedan pristup praćenju rizika treće strane pružatelja ključnih IKT usluga na razini Unije. S obzirom na prethodno navedeno, zakonodavna tijela Unije možda će željeti razmotriti dodjeljivanje posebnih ovlasti za provedbu zakonskim nadzornim tijelima u odnosu na treće strane pružatelje ključnih usluga IKT-a, uzimajući u obzir ograničenja koja nameće doktrina *Meroni*, što je Sud Europske unije djelomično ublažio u svojoj presudi u slučaju ESMA-e ([99]).

([93]) Vidi članak 29. Prijedloga uredbe.
([94]) Vidi članak 29. stavak 3. Prijedloga uredbe.
([95]) Vidi članak 35. Prijedloga uredbe.
([96]) Vidi članak 39. stavak 1. Prijedloga uredbe.
([97]) Vidi članak 29. stavak 4. i članak 37. Prijedloga uredbe.
([98]) Vidi članak 37. stavak 3. Prijedloga uredbe.
([99]) Vidi presudu Suda (Veliko vijeće), 22. siječnja 2014. Ujedinjena Kraljevina Velike Britanije i Sjeverne Irske v.Europski parlament i Vijeće Europske unije, Uredba (EU) br. 236/2012 — predmet C-270/12.

Kada ESB predlaže izmjenu Prijedloga uredbe, konkretni prijedlozi izmjena navedeni su u posebnom tehničkom radnom dokumentu kojem je u tu svrhu priloženo obrazloženje. Tehnički radni dokument dostupan je na engleskom jeziku na mrežnim stranicama EUR-Lexa.

Sastavljeno u Frankfurtu na Majni 4. lipnja 2021.

Predsjednica ESB-a
Christine LAGARDE