I.

(Zakonodavni akti)

UREDBE

UREDBA (EU) 2022/2554 EUROPSKOG PARLAMENTA I VIJEĆA

od 14. prosinca 2022.

o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europske središnje banke ([1]),

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ([2]),

u skladu s redovnim zakonodavnim postupkom ([3]),

budući da:

(1) U digitalnom se dobu složeni sustavi koji služe svakodnevnim aktivnostima temelje na informacijskoj i komunikacijskoj tehnologiji (IKT). Ona je zaslužna za funkcioniranje naših gospodarstava u ključnim sektorima, uključujući financijski sektor, i unapređuje funkcioniranja unutarnjeg tržišta. Sve veća digitalizacija i međusobna povezanost povećavaju i IKT rizik, što društvo u cjelini, a posebno financijski sustav, čini osjetljivijim na kiberprijetnje ili poremećaje u području IKT-a. Iako su sveprisutna upotreba sustava IKT-a i visok stupanj digitalizacije i povezivosti u današnje vrijeme ključne značajke aktivnosti financijskih subjekata u Uniji, njihovu digitalnu otpornost tek treba ojačati i integrirati u njihove šire operativne okvire.

(2) Upotreba IKT-a posljednjih je desetljeća u toj mjeri stekla središnju ulogu u pružanju financijskih usluga da je sada izuzetno važna za uobičajeno dnevno poslovanje svih financijskih subjekata. Digitalizacijom su sada obuhvaćena, na primjer, plaćanja, čiji se gotovinski ili papirnati oblik sve više zamjenjuje digitalnim rješenjima, te poravnanje i namira vrijednosnih papira, elektroničko i algoritamsko trgovanje, poslovi kreditiranja i financiranja, uzajamno kreditiranje, kreditni rejting, upravljanje potraživanjima i poslovi pozadinskih ureda. Upotreba IKT-a preobrazila je i sektor osiguranja, od pojave posrednika u osiguranju koji na temelju tehnologija u sektoru osiguranja (InsurTech)

([1]) SL C 343, 26.8.2021., str. 1.
([2]) SL C 155, 30.4.2021., str. 38.
([3]) Stajalište Europskog parlamenta od 10. studenoga 2022. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 28. studenoga 2022.

nude svoje usluge putem interneta do digitalnog preuzimanja rizika u osiguranju. Ne samo da su financije postale uglavnom digitalne u cijelom sektoru, nego je digitalizacija produbila i međusobne povezanosti i ovisnosti unutar financijskog sektora te u odnosu na infrastrukture trećih strana i treće strane koje su pružatelji usluga.

(3) U izvješću o sistemskom kiberriziku (2020.) Europski odbor za sistemske rizike (ESRB) potvrdio je da bi postojeći visoki stupanj međusobne povezanosti financijskih subjekata, financijskih tržišta i infrastruktura financijskog tržišta, a osobito međuovisnosti njihovih sustava IKT-a, mogao predstavljati sistemsku ranjivost jer bi se kiberincidenti mogli brzo proširiti s bilo kojeg od oko 22 000 financijskih subjekata u Uniji na cijeli financijski sustav, neovisno o zemljopisnim granicama. Ozbiljne povrede koje se dogode u području IKT-a u financijskom sektoru ne utječu samo na izolirane financijske subjekte. One olakšavaju i širenje lokaliziranih ranjivosti po svim kanalima financijskog prijenosa i mogle bi imati negativne posljedice na stabilnost financijskog sustava Unije, kao što su pad likvidnosti i opći gubitak povjerenja i pouzdanja u financijska tržišta.

(4) U proteklih nekoliko godina IKT rizik privlači pozornost međunarodnih, Unijinih i nacionalnih oblikovatelja politika, regulatornih tijela i tijela za normizaciju koji nastoje unaprijediti digitalnu otpornost, utvrditi standarde i koordinirati regulatorni ili nadzorni rad. Na međunarodnoj razini cilj je Bazelskog odbora za nadzor banaka, Odbora za platne i tržišne infrastrukture, Odbora za financijsku stabilnost, Instituta za financijsku stabilnost te skupina G-7 i G-20 pružiti nadležnim tijelima i tržišnim operaterima u različitim jurisdikcijama alate za poboljšanje otpornosti njihovih financijskih sustava. Taj se rad temelji i na potrebi za uzimanjem u obzir IKT rizika u kontekstu snažno povezanog globalnog financijskog sustava i postizanja veće usklađenosti relevantnih najboljih praksi.

(5) Unatoč Unijinim i nacionalnim ciljanim politikama i zakonodavnim inicijativama IKT rizik i dalje je problem za operativnu otpornost, uspješnost i stabilnost financijskog sustava Unije. Reformama koje su uslijedile nakon financijske krize iz 2008. prvenstveno je povećana financijska otpornost financijskog sektora Unije, a njihov cilj bile su zaštita konkurentnosti i stabilnosti Unije s gospodarskog i bonitetnog aspekta te aspekta ponašanja na tržištu. Iako su sigurnost IKT-a i digitalna otpornost dio operativnog rizika, nakon financijske krize nije im posvećena prevelika pozornost u regulatornim planovima pa su se razvile samo u nekim područjima političkog i regulatornog okruženja Unije za financijske usluge ili samo u nekoliko država članica.

(6) U Komunikaciji od 8. ožujka 2018. pod naslovom „Akcijski plan za financijske tehnologije: za konkurentniji i inovativniji europski financijski sektor” Komisija je istaknula da je izuzetno važno jačati otpornost financijskog sektora Unije, među ostalim i u operativnom smislu, kako bi se osigurali njegova tehnološka sigurnost i dobro funkcioniranje, brz oporavak od povreda i incidenata u području IKT-a, a time u konačnici omogućilo djelotvorno i neometano pružanje financijskih usluga u cijeloj Uniji, među ostalim i u stresnim okolnostima, uz istodobno očuvanje povjerenja potrošača i povjerenja u tržište.

(7) U travnju 2019. europsko nadzorno tijelo (Europsko nadzorno tijelo za bankarstvo, EBA) osnovano Uredbom (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([4]), europsko nadzorno tijelo (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), („EIOPA”) osnovano Uredbom (EU) br. 1094/2010 Europskog parlamenta i Vijeća ([5]) i Europsko nadzorno tijelo (Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala, „ESMA”)

([4]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12.).

([5]) Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48.).

osnovano Uredbom (EU) br. 1095/2010 Europskog parlamenta i Vijeća ([6]) (zajedno poznata kao „europska nadzorna tijela") zajednički su objavili tehnički savjet u kojem se poziva na usklađen pristup IKT riziku u području financija i preporučuje razmjerno jačanje digitalne operativne otpornosti industrije financijskih usluga putem sektorske inicijative Unije.

(8) Financijski sektor Unije uređen je jedinstvenim pravilima i Europskim sustavom financijskog nadzora. Unatoč tome, odredbe o digitalnoj operativnoj otpornosti i sigurnosti IKT-a još nisu potpuno i dosljedno usklađene iako je digitalna operativna otpornost ključna za financijsku stabilnost i cjelovitost tržišta u digitalnom dobu i nije manje važna od, na primjer, zajedničkih bonitetnih standarda ili standarda ponašanja na tržištu. Stoga bi trebalo razviti jedinstvena pravila i sustav nadzora kako bi se njima obuhvatila i digitalna operativna otpornost, i to jačanjem mandata nadležnih tijela kako bi mogla nadzirati upravljanje IKT rizikom u financijskom sektoru radi zaštite cjelovitosti i učinkovitosti unutarnjeg tržišta i olakšavanja njegova urednog funkcioniranja.

(9) Zakonodavne neusklađenosti i neujednačeni nacionalni regulatorni ili nadzorni pristupi u pogledu IKT rizika prepreka su funkcioniranju unutarnjeg tržišta za financijske usluge i onemogućavaju neometano ostvarivanje slobode poslovnog nastana i pružanje usluga za financijske subjekte koji posluju prekogranično. Tržišno natjecanje među financijskim subjektima iste vrste koji posluju u različitim državama članicama moglo bi također biti narušeno. To je posebno slučaj u područjima u kojima je usklađivanje na razini Unije vrlo ograničeno, kao što je testiranje digitalne operativne otpornosti, ili ne postoji, kao što je praćenje IKT rizika povezanog s trećim stranama. Neusklađenosti koje proizlaze iz predviđenih kretanja na nacionalnoj razini mogle bi stvoriti dodatne prepreke funkcioniranju unutarnjeg tržišta na štetu sudionika na tržištu i financijske stabilnosti.

(10) Budući da se odredbe povezane s IKT rizicima do današnjeg vremena samo djelomično razmatralo na razini Unije, postoje praznine ili preklapanja u važnim područjima, kao što su izvješćivanje o IKT incidentima i testiranje digitalne operativne otpornosti, te nedosljednosti koje proizlaze iz novih međusobno različitih nacionalnih pravila ili troškovno neučinkovite primjene preklapajućih pravila. To osobito šteti korisnicima koji se intenzivno koriste IKT-om, poput financijskog sektora, jer tehnološki rizici ne poznaju granice, a financijski sektor nudi širok spektar prekograničnih usluga unutar i izvan Unije. Pojedinačni financijski subjekti koji posluju prekogranično ili imaju nekoliko odobrenja za rad (npr. financijski subjekt može imati odobrenje za rad kao banka, kao investicijsko društvo i kao institucija za platni promet, pri čemu svako odobrenje izdaje drugo nadležno tijelo u jednoj ili više država članica) izloženi su operativnim rizicima pri samostalnom i dosljednom troškovno učinkovitom nošenju s IKT rizikom i ublažavanju negativnih učinaka IKT incidenata.

(11) Budući da jedinstvena pravila nisu popraćena sveobuhvatnim okvirom za IKT ili operativne rizike, potrebno je dodatno uskladiti ključne zahtjeve u pogledu digitalne operativne otpornosti za sve financijske subjekte. Razvoj sposobnosti u području IKT-a i ukupna otpornost financijskih subjekata, na temelju tih ključnih zahtjeva, s ciljem postizanja otpornosti na operativne ispade, pomogli bi očuvanju stabilnosti i cjelovitosti financijskih tržišta u Uniji, te bi tako doprinijeli osiguranju visoke razine zaštite ulagatelja i potrošača u Uniji. Budući da je cilj ove Uredbe doprinos neometanom funkcioniranju unutarnjeg tržišta, ona bi se trebala temeljiti na odredbama članka 114. Ugovora o funkcioniranju Europske unije (UFEU) kako se tumače u skladu s dosljednom sudskom praksom Suda Europske unije (Sud).

(12) Cilj je ove Uredbe konsolidirati i unaprijediti zahtjeve u pogledu IKT rizika kao dio zahtjeva u pogledu operativnog rizika koji su se dosad zasebno razmatrali u različitim pravnim aktima Unije. Iako su tim aktima obuhvaćene glavne kategorije financijskih rizika (npr. kreditni rizik, tržišni rizik, kreditni rizik druge ugovorne strane i rizik likvidnosti, rizik ponašanja na tržištu), njima u vrijeme njihova donošenja nisu sveobuhvatno obrađene sve komponente operativne otpornosti. Pravila za operativne rizike koja su dodatno razrađena u tim pravnim aktima Unije često su se temeljila na tradicionalnom kvantitativnom pristupu nošenja s rizikom (to jest određivanje kapitalnog zahtjeva za pokrivanje IKT rizika) te nisu bila ciljana kvalitativna pravila za sposobnosti za zaštitu, otkrivanje, ograničenje,

([6]) Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84.).

oporavak i popravak u slučaju IKT incidenata ili za sposobnosti za izvješćivanje i digitalno testiranje. Ti akti prvenstveno su se odnosili na temeljna pravila o bonitetnom nadzoru, cjelovitosti tržišta ili ponašanju na njemu te na ažuriranje tih pravila. Konsolidiranjem i ažuriranjem različitih pravila o IKT rizicima, sve odredbe koje se odnose na digitalne rizike u financijskom sektoru trebale bi se prvi put dosljedno objediniti u jedinstveni zakonodavni akt. Stoga se ovom Uredbom popunjavaju praznine ili uklanjaju nedosljednosti u nekim prethodnim pravnim aktima, među ostalim u vezi s terminologijom koja se u njima upotrebljava, te se izričito upućuje na IKT rizik putem ciljanih pravila o sposobnostima za upravljanje IKT rizicima, izvješćivanju o incidentima, testiranju operativne otpornosti i praćenju IKT rizika povezanog s trećim stranama. Ovom bi se Uredbom stoga trebala podići i svijest o IKT rizicima i uvažiti činjenica da IKT incidenti i pomanjkanje operativne otpornosti mogu ugroziti stabilnost financijskih subjekata. Konsolidiranjem i ažuriranjem različitih pravila o IKT rizicima, sve odredbe koje se odnose na digitalne rizike u financijskom sektoru trebale bi se prvi put dosljedno objediniti u jedinstveni zakonodavni akt. Stoga se ovom Uredbom popunjavaju praznine ili uklanjaju nedosljednosti u nekim prethodnim pravnim aktima, među ostalim u vezi s terminologijom koja se u njima upotrebljava, te se izričito upućuje na IKT rizik putem ciljanih pravila o sposobnostima za upravljanje IKT rizicima, izvješćivanju o incidentima, testiranju operativne otpornosti i praćenju IKT rizika povezanog s trećim stranama. Ovom bi se Uredbom stoga trebala podići i svijest o IKT rizicima i uvažiti činjenica da IKT incidenti i pomanjkanje operativne otpornosti mogu ugroziti stabilnost financijskih subjekata.

(13) Financijski subjekti trebali bi u nošenju s IKT rizikom slijediti isti pristup i ista pravila koja se temelje na načelima, pri čemu bi uzimali u obzir njihovu veličinu i ukupni profil rizičnosti te prirodu, opseg i složenost svojih usluga, aktivnosti i poslovanja. Dosljednost doprinosi povećanju povjerenja u financijski sustav te očuvanju njegove stabilnosti, osobito u razdoblju izrazitog oslanjanja na sustave, platforme i infrastrukture IKT-a, što podrazumijeva povećani digitalni rizik. Pridržavanjem osnovne kiberhigijene trebalo bi se ujedno izbjeći nastajanje velikih troškova za gospodarstvo svođenjem učinka i troškova poremećaja u radu IKT-a na najmanju moguću mjeru.

(14) Uredbom se doprinosi smanjenju regulatorne složenosti, promiče konvergencija nadzora, povećava pravna sigurnost i istodobno doprinosi ograničavanju troškova osiguravanja usklađenosti, osobito financijskih subjekata koji posluju prekogranično, te smanjenju narušavanja tržišnog natjecanja. Odabir uredbe za uspostavu zajedničkog okvira za digitalnu operativnu otpornost financijskih subjekata stoga je najprimjereniji način za jamčenje homogene i dosljedne primjene svih komponenti upravljanja IKT rizicima u financijskom sektoru Unije.

(15) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća ([7]) bila je prvi horizontalni okvir za kibersigurnost donesen na razini Unije, koji se primjenjuje i na tri vrste financijskih subjekata, to jest kreditne institucije, mjesta trgovanja i središnje druge ugovorne strane. Međutim, s obzirom na to da se Direktivom (EU) 2016/1148 utvrđuje mehanizam identifikacije operatora ključnih usluga na nacionalnoj razini, države članice identificirale su samo određene kreditne institucije, mjesta trgovanja i središnje druge ugovorne strane koje su u praksi obuhvaćene njezinim područjem primjene i stoga su dužne ispunjavati zahtjeve u pogledu sigurnosti IKT-a i obavješćivanja o incidentima koji su u njoj utvrđeni. Direktivom (EU) 2022/2555 Europskog parlamenta i Vijeća ([8]) utvrđuje se jedinstveni kriterij za određivanje subjekata koji su obuhvaćeni njezinim područjem primjene (pravilo o maksimalnoj veličini), dok su tri vrste financijskih subjekata i dalje zadržane u području njezine primjene.

(16) Međutim, budući da se ovom Uredbom podiže razina usklađenosti različitih komponenti digitalne otpornosti tako što se uvode zahtjevi u pogledu upravljanja IKT rizicima i izvješćivanja o IKT incidentima koji su stroži od onih utvrđenih u postojećem pravu Unije o financijskim uslugama, tom višom razinom poboljšava se i usklađenost u usporedbi sa zahtjevima utvrđenima u Direktivi (EU) 2022/2555 Stoga je ova Uredba *lex specialis* u odnosu na Direktivu (EU) 2022/2555. Istodobno je iznimno važno očuvati čvrstu vezu između financijskog sektora i horizontalnog okvira Unije za kibersigurnost, kako je trenutačno utvrđen u Direktivi (EU) 2022/2555, kako bi se osigurala dosljednost sa strategijama kibersigurnosti koje su države članice donijele i omogućilo informiranje financijskih nadzornih tijela o kiberincidentima koji utječu na druge sektore obuhvaćene tom direktivom.

([7]) 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.).

([8]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (vidjeti stranicu 80.. ovoga Službenog lista).

(17) U skladu s člankom 4. stavkom 2. Ugovora o Europskoj uniji i ne dovodeći u pitanje sudsko preispitivanje koje provodi Sud, ova Uredba ne bi trebala utjecati na odgovornost država članica u pogledu temeljnih državnih funkcija koje se odnose na javnu sigurnost, obranu i zaštitu nacionalne sigurnosti, na primjer u pogledu pružanja informacija koje bi bilo protivno zaštiti nacionalne sigurnosti.

(18) Kako bi se omogućilo međusektorsko učenje i djelotvorno iskoristila iskustva iz drugih sektora pri suočavanju s kiberprijetnjama, financijski subjekti iz Direktive (EU) 2022/2555 trebali bi ostati dio „ekosustava" te direktive (na primjer skupina za suradnju i timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)). Europska nadzorna tijela i nacionalna nadležna tijela trebala bi moći sudjelovati u raspravama o strateškim politikama i tehničkom radu Skupine za suradnju iz te direktive, razmjenjivati informacije i dodatno surađivati s jedinstvenim kontaktnim točkama imenovanima ili uspostavljenima u skladu s tom direktivom. Nadležna tijela iz ove Uredbe trebala bi se također savjetovati i surađivati s CSIRT-ovima. Nadležna tijela trebala bi također moći zatražiti tehničke savjete od nadležnih tijela imenovanih ili uspostavljenih u skladu s Direktivom (EU) 2022/2555 i uspostaviti aranžmane za suradnju kojima se nastoje osigurati djelotvorni i brzi koordinacijski mehanizmi.

(19) S obzirom na snažnu povezanost digitalne i fizičke otpornosti financijskih subjekata, u ovoj Uredbi i u Direktivi (EU) 2022/2557 Europskog parlamenta i Vijeća ([9]) potreban je dosljedan pristup u pogledu otpornosti kritičnih subjekata. S obzirom na to da se obvezama upravljanja IKT rizicima i obvezama izvješćivanja o IKT rizicima koje su obuhvaćene ovom Uredbom na sveobuhvatan način pristupa fizičkoj otpornosti financijskih subjekata, obveze utvrđene u poglavljima III. i IV. Direktive (EU) 2022/2557 ne bi se trebale primjenjivati na financijske subjekte obuhvaćene područjem primjene te direktive.

(20) Pružatelji usluga računalstva u oblaku jedna su od kategorija digitalne infrastrukture obuhvaćene Direktivom (EU) 2022/2555. Nadzorni okvir Unije („nadzorni okvir") uspostavljen ovom Uredbom primjenjuje se na sve ključne treće strane pružatelje IKT usluga, uključujući pružatelje usluga računalstva u oblaku koji financijskim subjektima pružaju IKT usluge, te bi ga trebalo smatrati dopunom nadzoru koji se provodi na temelju Direktive (EU) 2022/2555. Osim toga, nadzornim okvirom uspostavljenim ovom Uredbom trebalo bi obuhvatiti pružatelje usluga računalstva u oblaku jer ne postoji horizontalni okvir Unije o uspostavi tijela za digitalni nadzor.

(21) Kako bi se očuvala potpuna kontrola nad IKT rizikom, financijski subjekti moraju imati sveobuhvatne kapacitete kojima se omogućuje snažno i djelotvorno upravljanje IKT rizicima, kao i posebne mehanizme i politike za postupanje u vezi sa svim IKT incidentima i izvješćivanje o značajnim IKT incidentima. Isto tako, financijski subjekti trebali bi uspostaviti politike za testiranje sustava, kontrola i procesa u području IKT-a, kao i za upravljanje IKT rizikom povezanim s trećim stranama. Trebalo bi povećati polaznu digitalnu operativnu otpornost financijskih subjekata te istodobno također omogućiti razmjernu primjenu zahtjevâ za određene financijske subjekte, posebno mikropoduzeća, kao i za financijske subjekte koji podliježu pojednostavnjenom okviru za upravljanje IKT rizicima. Kako bi se olakšao učinkovit nadzor institucija za strukovno mirovinsko osiguranje koji je razmjeran i kojim se pristupa rješavanju potrebe za smanjenjem administrativnog opterećenja nadležnih tijela, relevantnim nacionalnim nadzornim aranžmanima u pogledu takvih financijskih subjekata trebalo bi uzeti u obzir njihovu veličinu i ukupni profil rizičnosti te prirodu, opseg i složenost njihovih usluga, aktivnosti i poslovanja, čak i ako su premašeni relevantni pragovi utvrđeni u članku 5. Direktive (EU) 2016/2341 Europskog parlamenta i Vijeća ([10]). Posebno, aktivnosti nadzora trebale bi se u prvom redu usredotočiti na potrebu za nošenjem s ozbiljnim rizicima povezanima s upravljanjem IKT rizicima određenog subjekta.

([9]) Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (vidjeti stranicu 164.. ovoga Službenog lista).

([10]) Direktiva (EU) 2016/2341 Europskog parlamenta i Vijeća od 14. prosinca 2016. o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje (SL L 354, 23.12.2016., str. 37.).

Nadležna tijela također bi trebala zadržati oprezan, ali razmjeran pristup u vezi s nadzorom institucija za strukovno mirovinsko osiguranje koje, u skladu s člankom 31. Direktive 2016/2341, eksternaliziraju znatan dio svojih osnovnih aktivnosti, kao što su upravljanje imovinom, aktuarski izračuni, računovodstvo i upravljanje podacima.

(22) Pragovi i taksonomije za izvješćivanje o IKT incidentima znatno se razlikuju na nacionalnoj razini. Iako bi se zajednički dogovor mogao postići na temelju relevantnog rada Agencije Europske unije za kibersigurnost (ENISA) osnovane Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća ([11]) i Skupine za suradnju iz Direktive (EU) 2022/2555, i dalje postoje ili se mogu pojaviti različiti pristupi utvrđivanju pragova i primjeni taksonomija za preostale financijske subjekte. Zbog tih razlika financijski subjekti moraju ispuniti višestruke zahtjeve, osobito kad posluju u nekoliko država članica i kad su dio financijske grupe. Štoviše, takve razlike mogu ometati izradu dodatnih ujednačenih ili centraliziranih mehanizama Unije kojima bi se ubrzao proces izvješćivanja te podržala brza i neometana razmjena informacija među nadležnim tijelima, što je ključno za nošenje s IKT rizikom u slučaju opsežnih napada s mogućim sistemskim posljedicama.

(23) Kako bi se smanjilo administrativno opterećenje i moguće udvostručivanje obveza izvješćivanja za određene financijske subjekte, zahtjev u vezi s izvješćivanjem o incidentima na temelju Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća ([12]) trebao bi se prestati primjenjivati na pružatelje platnih usluga koji su obuhvaćeni područjem primjene ove Uredbe. Slijedom toga, kreditne institucije, institucije za elektronički novac, institucije za platni promet i pružatelji usluga pružanja informacija o računu, kako je navedeno u članku 33. stavku 1. te direktive, trebali bi od datuma primjene ove Uredbe izvješćivati, na temelju ove Uredbe, o svim operativnim ili sigurnosnim incidentima povezanima s plaćanjem o kojima se prethodno izvješćivalo na temelju te direktive, neovisno o tome jesu li takvi incidenti povezani s IKT-om.

(24) Kako bi se nadležnim tijelima omogućilo da ispune nadzorne zadaće dobivanjem potpunog uvida u prirodu, učestalost, značaj i učinak IKT incidenata i da bi se unaprijedila razmjena informacija među relevantnim tijelima javne vlasti, uključujući tijela za izvršavanje zakonodavstva i sanacijska tijela, ovom Uredbom trebalo bi utvrditi pouzdan sustav izvješćivanja o IKT incidentima, pri čemu se relevantnim zahtjevima popunjavaju postojeće praznine u pravu o financijskim uslugama i uklanjaju postojeća preklapanja i udvostručavanja radi smanjenja troškova. Neophodno je uskladiti sustav izvješćivanja o IKT incidentima tako da se sve financijske subjekte obveže da svojim nadležnim tijelima podnose izvješća putem jedinstvenog racionaliziranog okvira kako je utvrđen u ovoj Uredbi. Osim toga, europska nadzorna tijela trebalo bi ovlastiti za daljnju razradu relevantnih elemenata okvira za izvješćivanje o IKT incidentima, kao što su taksonomija, rokovi, skupovi podataka, obrasci i primjenjivi pragovi. Kako bi se osigurala potpuna usklađenost s Direktivom (EU) 2022/2555, financijskim subjektima trebalo bi omogućiti da na dobrovoljnoj osnovi obavijeste relevantno nadležno tijelo o ozbiljnim kiberprijetnjama kad smatraju da je kiberprijetnja relevantna za financijski sustav, korisnike usluga ili klijente.

(25) U određenim financijskim podsektorima razvijeni su zahtjevi za testiranje digitalne operativne otpornosti kojima se utvrđuju okviri koji nisu uvijek potpuno usklađeni. To dovodi do mogućeg udvostručavanja troškova za prekogranične financijske subjekte, a uzajamno priznavanje rezultata testiranja digitalne operativne otpornosti čini složenim, što pak može dovesti do fragmentiranja unutarnjeg tržišta.

([11]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

([12]) Direktiva (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.).

(26) Osim toga, ako testiranje IKT-a nije propisano, ranjivosti ostaju neotkrivene i imaju za posljedicu izlaganje financijskog subjekta IKT riziku te, u konačnici, dovode do većeg rizika za stabilnost i cjelovitost financijskog sektora. Bez intervencije Unije testiranje digitalne operativne otpornosti i dalje bi bilo neujednačeno i ne bi bilo sustava uzajamnog priznavanja rezultata testiranja IKT-a u različitim jurisdikcijama. Osim toga, s obzirom na to da nije vjerojatno da bi drugi financijski podsektori u relevantnom opsegu usvojili programe testiranja, propustili bi potencijalne koristi okvira za testiranje, kao što su otkrivanje ranjivosti i rizika u području IKT-a i testiranje obrambenih sposobnosti i kontinuiteta poslovanja, kojim se doprinosi povećanju povjerenja potrošača, dobavljača i poslovnih partnera. Kako bi se ta preklapanja, razlike i odstupanja uklonili, potrebno je utvrditi pravila za koordinirani režim testiranja i time olakšati uzajamno priznavanje naprednog testiranja za financijske subjekte koji ispunjavaju kriterije utvrđene u ovoj Uredbi.

(27) Oslanjanje financijskih subjekata na upotrebu IKT usluga djelomično je potaknuto njihovom potrebom da se prilagode novom konkurentnom digitalnom globalnom gospodarstvu, da povećaju učinkovitost svojeg poslovanja i odgovore na potražnju potrošača. Priroda i opseg tog oslanjanja neprestano su se mijenjali proteklih godina, što je dovelo do smanjenja troškova financijskog posredovanja te omogućilo širenje i skalabilnost poslovanja pri uvođenju financijskih aktivnosti, ali i ponudu širokog spektra alata IKT-a za upravljanje složenim unutarnjim procesima.

(28) Široka upotreba IKT usluga očituje se u složenim ugovornim aranžmanima, pri čemu financijski subjekti često nailaze na poteškoće u postizanju dogovora prilikom pregovaranja o ugovornim uvjetima koji su prilagođeni bonitetnim standardima ili drugim regulatornim zahtjevima kojima financijski subjekti podliježu, ili u ostvarivanju određenih prava, kao što su prava pristupa ili revizije, čak i kad su ta prava dio njihovih ugovornih aranžmana. Štoviše, mnogim se od tih ugovornih aranžmana ne predviđaju dostatne mjere zaštite kojima bi se omogućilo cjelovito praćenje podugovaranja, čime se financijskom subjektu uskraćuje mogućnost procjene povezanih rizika. Osim toga, s obzirom na to da treće strane pružatelji IKT usluga često pružaju standardizirane usluge različitim vrstama klijenata, takvi ugovorni aranžmani nisu uvijek odgovarajuće prilagođeni pojedinačnim ili posebnim potrebama subjekata u financijskom sektoru.

(29) Iako pravo Unije o financijskim uslugama sadržava određena opća pravila o eksternalizaciji, praćenje ugovorne dimenzije nije u potpunosti ugrađeno u pravo Unije. Budući da ne postoje jasni i specijalizirani standardi Unije koji bi se primjenjivali na ugovorne aranžmane sklopljene s trećim stranama pružateljima IKT usluga, vanjski izvor IKT rizika nije sveobuhvatno obrađen. Stoga je potrebno utvrditi određena ključna načela za usmjeravanje financijskih subjekata u upravljanju IKT rizikom povezanim s trećim stranama, koja su od posebne važnosti kad se financijski subjekti oslanjaju na treće strane pružatelje IKT usluga kako bi poduprli svoje ključne ili važne funkcije. Ta bi načela trebala biti popraćena skupom temeljnih ugovornih prava u odnosu na nekoliko elemenata u izvršenju i raskidu ugovornih aranžmana s ciljem pružanja određenih minimalnih zaštitnih mjera kojima bi se ojačala sposobnost financijskih subjekata da djelotvorno prate svaki IKT rizik koji se pojavljuje na razini trećih strana pružatelja usluga. Tim se načelima nadopunjuje sektorsko pravo koje se primjenjuje na eksternalizaciju.

(30) Trenutačno je očito određeno pomanjkanje homogenosti i konvergencije u pogledu praćenja IKT rizika povezanog s trećim stranama i ovisnosti o trećim stranama u području IKT-a. Unatoč- naporima za rješavanje pitanja eksternalizacije, kao što su Smjernice EBA-e o eksternalizaciji iz 2019. i Smjernice ESMA-e za eksternalizaciju usluga računalstva u oblaku iz 2021., šire pitanje sprečavanja sistemskog rizika koji bi se mogao pojaviti zbog izloženosti financijskog sektora ograničenom broju ključnih trećih strana pružatelja IKT usluga nije dostatno obrađeno u pravu Unije. Pomanjkanje pravila na razini Unije dodatno je naglašeno nepostojanjem nacionalnih pravila o ovlastima i alatima koji bi financijskim nadzornim tijelima omogućili bolje razumijevanje ovisnosti o trećim stranama u području IKT-a i primjereno praćenje rizika koji proizlaze iz koncentracije ovisnosti o trećim stranama u području IKT-a.

(31) Uzimajući u obzir mogući sistemski rizik koji prati sve češću praksu eksternalizacije poslova i koncentraciju IKT usluga trećih strana te vodeći računa o nedostatnosti nacionalnih mehanizama u osiguravanju odgovarajućih alata financijskim nadzornim tijelima za kvantificiranje, kvalificiranje i otklanjanje posljedica IKT rizika koji nastaje kod ključnih trećih strana pružatelja IKT usluga, potrebno je uspostaviti odgovarajući nadzorni okvir kojim se omogućuje kontinuirano praćenje aktivnosti trećih strana pružatelja IKT usluga koji su ključne treće strane pružatelji IKT usluga financijskim subjektima, osiguravajući pritom povjerljivost i sigurnost klijenata koji nisu financijski subjekti. Iako pružanje IKT usluga unutar grupe podrazumijeva posebne rizike i koristi, ono se ne bi trebalo automatski smatrati manje rizičnim od pružanja IKT usluga od strane pružatelja izvan financijske grupe te bi stoga trebalo podlijegati istom regulatornom okviru. Međutim, ako se IKT usluge pružaju unutar iste financijske grupe, financijski subjekti mogli bi imati višu razinu kontrole nad pružateljima unutar grupe, što bi trebalo uzeti u obzir u ukupnoj procjeni rizika.

(32) Budući da rizik IKT-a postaje sve složeniji i sofisticiraniji, dobre mjere za otkrivanje i sprečavanje IKT rizika u velikoj mjeri ovise o redovitoj razmjeni saznanja o prijetnjama i ranjivostima među financijskim subjektima. Razmjenom informacija doprinosi se jačanju svijesti o kiberprijetnjama. Time se pak povećava kapacitet financijskih subjekata da spriječe da kiberprijetnje postanu stvarni IKT incidenti te se financijskim subjektima omogućuje da djelotvornije ograniče učinak IKT incidenata i brže se oporave. U nedostatku smjernica na razini Unije čini se da nekoliko čimbenika sprečava takvu razmjenu saznanja, osobito nesigurnost u pogledu usklađenosti s pravilima o zaštiti podataka, zaštiti od monopola i odgovornosti.

(33) Osim toga, zbog nedoumica u vezi s vrstama informacija koje se smiju dijeliti s drugim sudionicima na tržištu ili s nenadzornim tijelima (kao što je ENISA u analitičke svrhe ili Europol u svrhu kaznenog progona) uskraćuju se korisne informacije. Stoga su opseg i kvaliteta razmjene informacija trenutačno i dalje ograničeni i rascjepkani, a relevantne razmjene odvijaju se uglavnom na lokalnoj razini (u okviru nacionalnih inicijativa) te ne postoje dosljedni mehanizmi razmjene informacija na razini Unije koji su prilagođeni potrebama integriranog financijskog sustava. Stoga je važno ojačati te komunikacijske kanale.

(34) Financijske subjekte trebalo bi poticati na međusobnu razmjenu informacija i saznanja o kiberprijetnjama te na zajedničko iskorištavanje znanja i praktičnog iskustva svakog od njih na strateškoj, taktičkoj i operativnoj razini s ciljem unapređenja njihovih sposobnosti za odgovarajuću procjenu, praćenje, obranu i odgovor u pogledu kiberprijetnji, sudjelovanjem u aranžmanima za razmjenu informacija. Stoga je potrebno omogućiti uspostavu mehanizama dobrovoljne razmjene informacija na razini Unije koji bi, kad djeluju u pouzdanim okruženjima, pomogli zajednici financijske industrije da spriječi i zajednički odgovori na kiberprijetnje brzim ograničenjem širenja IKT rizika i onemogućivanjem eventualnog širenja zaraze putem financijskih kanala. Ti bi mehanizmi trebali biti usklađeni s primjenjivim pravilima prava tržišnog natjecanja Unije navedenima u Komunikaciji Komisije od 14. siječnja 2011. pod naslovom „Smjernice o primjenjivosti članka 101. Ugovora o funkcioniranju Europske unije na sporazume o horizontalnoj suradnji” i pravilima Unije o zaštiti podataka, osobito s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća ([13]). Trebali bi djelovati na temelju primjene jedne ili više pravnih osnova utvrđenih u članku 6. te uredbe, na primjer u kontekstu obrade osobnih podataka za potrebe legitimnog interesa voditelja obrade ili treće strane, kako je navedeno u članku 6. stavku 1. točki (f) te uredbe, kao i u kontekstu obrade osobnih podataka koja je nužna radi poštovanja pravne obveze voditelja obrade, koja je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade, kako je navedeno u članku 6. stavku 1. točki (c) odnosno točki (e) te uredbe.

([13]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

(35) Kako bi se održala visoka razina digitalne operativne otpornosti za cijeli financijski sektor i istodobno održao korak s tehnološkim razvojem, ovom bi se Uredbom trebalo nositi s rizicima koji proizlaze iz svih vrsta IKT usluga. U tu bi svrhu definiciju IKT usluga u kontekstu ove Uredbe trebalo tumačiti u širem smislu, tako da obuhvaća digitalne i podatkovne usluge koje se putem sustavâ IKT-a pružaju jednom ili više unutarnjih ili vanjskih korisnika na trajnoj osnovi. Ta bi definicija, na primjer, trebala uključivati takozvane OTT usluge (*„over the top" services*), koje pripadaju kategoriji elektroničkih komunikacijskih usluga. Njome se ne bi trebala obuhvatiti samo ograničena kategorija tradicionalnih analognih telefonskih usluga, odnosno usluge javne komutirane telefonske mreže (PSTN), usluge zemaljske linije, usluge koje se pružaju putem analognog (POTS) priključka, ili telefonske usluge fiksne linije.

(36) Iako je obuhvat predviđen ovom Uredbom doista širok, pri primjeni pravila o digitalnoj operativnoj otpornosti trebalo bi uzeti u obzir znatne razlike među financijskim subjektima u pogledu njihove veličine i ukupnog profila rizičnosti. Opće je načelo da bi financijski subjekti pri distribuiranju resursa i sposobnosti na provedbu okvira za upravljanje IKT rizicima trebali propisno uskladiti svoje potrebe u području IKT-a sa svojom veličinom i ukupnim profilom rizičnosti te prirodom, opsegom i složenošću svojih usluga, aktivnosti i poslovanja, a nadležna bi tijela pristup takvom distribuiranju i dalje trebala procjenjivati i preispitivati.

(37) Pružatelji usluga pružanja informacija o računu iz članka 33. stavka 1. Direktive (EU) 2015/2366 izričito su uključeni u područje primjene ove Uredbe, uzimajući u obzir specifičnu prirodu njihovih aktivnosti i rizike koji iz njih proizlaze. Osim toga, institucije za elektronički novac i institucije za platni promet izuzete na temelju članka 9. stavka 1. Direktive 2009/110/EZ Europskog parlamenta i Vijeća ([14]) i članka 32. stavka 1. Direktive (EU) 2015/2366 uključene su u područje primjene ove Uredbe čak i ako im nije izdano odobrenje za izdavanje elektroničkog novca u skladu s Direktivom 2009/110/EZ ili ako im nije izdano odobrenje za pružanje i izvršavanje platnih usluga u skladu s Direktivom (EU) 2015/2366. Međutim, poštanske žiro institucije iz članka 2. stavka 5. točke 3. Direktive 2013/36/EU Europskog parlamenta i Vijeća ([15]) isključene su iz područja primjene ove Uredbe. Nadležno tijelo za institucije za platni promet izuzeto na temelju Direktive (EU) 2015/2366, institucije za elektronički novac izuzete na temelju Direktive 2009/110/EZ i pružatelji usluga pružanja informacija o računu iz članka 33. stavka 1. Direktive (EU) 2015/2366 trebali bi biti nadležno tijelo imenovano u skladu s člankom 22. Direktive (EU) 2015/2366.

(38) Budući da bi veći financijski subjekti mogli imati na raspolaganju više resursa i da mogu brzo preusmjeriti sredstva na razvoj upravljačkih struktura i uspostavu različitih korporativnih strategija, samo bi financijske subjekte koji nisu mikropoduzeća u smislu ove Uredbe trebalo obvezati na uvođenje složenijih aranžmana za upravljanje. Takvi su subjekti bolje opremljeni osobito za uspostavu namjenskih upravljačkih funkcija za nadzor aranžmana s trećim stranama pružateljima IKT usluga ili upravljanje krizama, organizaciju svojeg upravljanja IKT rizicima u skladu s modelom „triju crta obrane", ili za uspostavu internog modela upravljanja rizicima i kontrole nad njima, te za podnošenje okvira za upravljanje IKT rizicima radi unutarnjih revizija.

(39) Na neke financijske subjekte primjenjuju se izuzeća ili oni podliježu vrlo blagom regulatornom okviru u sklopu relevantnog sektorskog prava Unije. Među takvim su financijskim subjektima upravitelji alternativnih investicijskih fondova iz članka 3. stavka 2. Direktive 2011/61/EU Europskog parlamenta i Vijeća ([16]), društva za osiguranje i društva za reosiguranje iz članka 4. Direktive 2009/138/EZ Europskog parlamenta i Vijeća ([17]) te institucije za strukovno mirovinsko osiguranje koje upravljaju mirovinskim programima koji zajedno nemaju više od ukupno 15

([14]) Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ (SL L 267, 10.10.2009., str. 7.).

([15]) Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama, 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.).

([16]) Direktiva 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i o izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010 (SL L 174, 1.7.2011., str. 1.).

([17]) Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).

članova. S obzirom na ta izuzeća ne bi bilo razmjerno uključiti takve financijske subjekte u područje primjene ove Uredbe. Osim toga, ovom se Uredbom uvažavaju posebnosti strukture tržišta posredovanja u osiguranju, zbog čega posrednici u osiguranju, posrednici u reosiguranju i sporedni posrednici u osiguranju koji se smatraju mikropoduzećima ili malim ili srednjim poduzećima ne bi trebali podlijegati ovoj Uredbi.

(40) Budući da su subjekti iz članka 2. stavka 5. točaka od 4. do 23. Direktive 2013/36/EU isključeni iz područja primjene te direktive, države članice trebale bi stoga moći odlučiti iz primjene ove Uredbe izuzeti takve subjekte koji se nalaze na njihovu državnom području.

(41) Slično tome, kako bi se ova Uredba uskladila s područjem primjene Direktive 2014/65/EU Europskog parlamenta i Vijeća ([18]), također je primjereno iz područja primjene ove Uredbe isključiti fizičke i pravne osobe iz članaka 2. i 3. te direktive kojima je dopušteno pružanje investicijskih usluga bez obveze pribavljanja odobrenja za rad na temelju Direktive 2014/65/EU. Međutim, člankom 2. Direktive 2014/65/EU iz područja primjene te direktive isključuju se i subjekti koji se smatraju financijskim subjektima za potrebe ove Uredbe, kao što su središnji depozitoriji vrijednosnih papira, subjekti za zajednička ulaganja ili društva za osiguranje i društva za reosiguranje. Isključenje iz područja primjene ove Uredbe osoba i subjekata iz članaka 2. i 3. te direktive ne bi trebalo obuhvaćati navedene središnje depozitorije vrijednosnih papira, subjekte za zajednička ulaganja ili društva za osiguranje i društva za reosiguranje.

(42) Prema sektorskom pravu Unije neki financijski subjekti podliježu blažim zahtjevima ili izuzećima zbog razloga povezanih s njihovom veličinom ili uslugama koje pružaju. Ta kategorija financijskih subjekata uključuje mala i nepovezana investicijska društva, male institucije za strukovno mirovinsko osiguranje koje dotična država članica može isključiti iz područja primjene Direktive (EU) 2016/2341 pod uvjetima utvrđenima u članku 5. te direktive i koje upravljaju mirovinskim programima koji nemaju više od ukupno 100 članova, kao i institucije izuzete na temelju Direktive 2013/36/EU. Stoga je, u skladu s načelom proporcionalnosti i kako bi se očuvao duh sektorskog prava Unije, primjereno i da se na te financijske subjekte primjenjuje pojednostavnjeni okvir za upravljanje IKT rizicima na temelju ove Uredbe. Proporcionalnost okvira za upravljanje IKT rizicima kojim su obuhvaćeni ti financijski subjekti ne bi se trebala mijenjati regulatornim tehničkim standardima koje trebaju razviti europska nadzorna tijela. Nadalje, u skladu s načelom proporcionalnosti, primjereno je da i institucije za platni promet iz članka 32. stavka 1. Direktive (EU) 2015/2366 i institucije za elektronički novac iz članka 9. Direktive 2009/110/EZ izuzete u skladu s nacionalnim pravom kojim se prenose ti pravni akti Unije podliježu pojednostavnjenom okviru za upravljanje IKT rizicima na temelju ove Uredbe, dok bi institucije za platni promet i institucije za elektronički novac koje nisu izuzete u skladu s odgovarajućim nacionalnim pravom kojim se prenosi sektorsko pravo Unije trebale biti usklađene s općim okvirom utvrđenim ovom Uredbom.

(43) Slično tome, od financijskih subjekata koji se smatraju mikropoduzećima ili koji podliježu pojednostavnjenom okviru za upravljanje IKT rizicima na temelju ove Uredbe ne bi trebalo zahtijevati da uspostave funkciju za praćenje svojih aranžmana o upotrebi IKT usluga sklopljenih s trećim stranama pružateljima IKT usluga ili imenuju člana višeg rukovodstva koji bi bio odgovoran za nadzor nad povezanim izloženostima rizicima i relevantnom dokumentacijom, da odgovornost za upravljanje IKT rizicima i nadzor nad njima dodijele kontrolnoj funkciji i osiguraju odgovarajuću razinu neovisnosti takve kontrolne funkcije kako bi se izbjegli sukobi interesa, da najmanje jednom godišnje dokumentiraju i preispitaju okvir za upravljanje IKT rizicima, da okvir za upravljanje IKT rizicima redovito podvrgavaju unutarnjoj reviziji, da nakon velikih promjena u infrastrukturama i procesima svojih mrežnih i informacijskih sustava provode dubinske procjene, da redovito provode analize rizika u zastarjelim IKT sustavima, da provedbu planova odgovora i oporavka u području IKT-a podvrgavaju neovisnom unutarnjem revizijskom pregledu, da imaju funkciju za upravljanje krizama, da prošire testiranje kontinuiteta poslovanja i planove odgovora i oporavka tako da njima obuhvate i scenarije prebacivanja s primarne infrastrukture IKT-a na redundantnu infrastrukturu i obrnuto, da nadležnim tijelima na njihov zahtjev dostavljaju procjenu agregiranih godišnjih troškova i gubitaka prouzročenih značajnim IKT incidentima, da održavaju redundantne kapacitete IKT-a, da

([18]) Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.).

obavješćuju nacionalna nadležna tijela o promjenama koje su provedene slijedom preispitivanja nakon IKT incidenata, da kontinuirano prate relevantna tehnološka dostignuća, da uspostave sveobuhvatan program testiranja digitalne operativne otpornosti kao sastavni dio okvira za upravljanje IKT rizicima predviđenog u ovoj Uredbi, ili da donesu i redovito preispituju strategiju o IKT riziku povezanom s trećim stranama. Uz navedeno, mikropoduzeća bi trebala imati obvezu procijeniti potrebu za očuvanjem takvih redundantnih kapaciteta IKT-a samo na temelju svojeg profila rizičnosti. Mikropoduzeća bi trebala imati pravo na fleksibilniji režim u pogledu programâ testiranja digitalne operativne otpornosti. Pri razmatranju vrste i učestalosti testiranja koje treba provesti, trebala bi na odgovarajući način postići ravnotežu između cilja očuvanja visoke digitalne operativne otpornosti, dostupnih resursa i njihova ukupnog profila rizičnosti. Mikropoduzeća i financijske subjekte na koje se primjenjuje pojednostavnjeni okvir za upravljanje IKT rizicima na temelju ove Uredbe trebalo bi izuzeti od zahtjeva da provode napredno testiranje IKT alata, sustava i procesa putem penetracijskog testiranja vođenog prijetnjama (TLPT) jer bi samo financijski subjekti koji ispunjavaju kriterije utvrđene u ovoj Uredbi trebali biti obvezni provoditi takvo testiranje. S obzirom na njihove ograničene sposobnosti mikropoduzeća bi se trebala moći dogovoriti s trećom stranom pružateljem IKT usluga o delegiranju prava financijskog subjekta na pristup, inspekcijski nadzor i reviziju neovisnoj trećoj strani koju treba imenovati treća strana pružatelj IKT usluga, pod uvjetom da financijski subjekt u svakom trenutku od odgovarajuće neovisne treće strane može zatražiti sve relevantne informacije i jamstva o radu treće strane pružatelja IKT usluga.

(44) Budući da bi samo oni financijski subjekti koji su identificirani za potrebe naprednog testiranja digitalne otpornosti trebali biti obvezni provoditi penetracijska testiranja vođena prijetnjama, administrativne postupke i financijske troškove povezane s provedbom takvih testova trebao bi snositi mali postotak financijskih subjekata.

(45) Kako bi se osigurala potpuna usklađenost i opća dosljednost poslovnih strategija financijskih subjekata s jedne strane te upravljanja IKT rizicima s druge strane, upravljačka tijela financijskih subjekata trebala bi obvezno imati središnju i aktivnu ulogu u usmjeravanju i prilagodbi okvira za upravljanje IKT rizicima i opće strategije digitalne operativne otpornosti. Pristup koji trebaju primijeniti upravljačka tijela ne bi se trebao usmjeriti samo na sredstva za osiguravanje otpornosti sustavâ IKT-a, nego bi također trebao obuhvaćati osoblje i procese politikama kojima se na svakoj razini poduzeća i među svim članovima osoblja podupire snažna osviještenost o kiberrizicima i obveza poštovanja stroge kiberhigijene na svim razinama. Krajnja odgovornost upravljačkog tijela za upravljanje IKT rizicima financijskog subjekta trebala bi biti glavno načelo tog sveobuhvatnog pristupa koje se pretače u kontinuiran angažman upravljačkog tijela u kontroli praćenja upravljanja IKT rizicima.

(46) Nadalje, načelo potpune i konačne odgovornosti upravljačkog tijela za upravljanje IKT rizicima financijskog subjekta usko je povezano s potrebom za osiguravanjem razine ulaganja povezanih s IKT-om i ukupnog proračuna za financijski subjekt, kojima bi se financijskom subjektu omogućilo da postigne visoku razinu digitalne operativne otpornosti.

(47) Ovom Uredbom, nadahnutom relevantnim međunarodnim, nacionalnim i industrijskim najboljim praksama, smjernicama, preporukama i pristupima za upravljanje kiberrizicima, promiče se niz načela koja olakšavaju cjelokupnu strukturu upravljanja IKT rizicima. Posljedično, dok god glavne sposobnosti koje su uspostavili financijski subjekti ispunjavaju različite funkcije u upravljanju IKT rizicima (utvrđivanje, zaštita i sprečavanje, otkrivanje, odgovor i oporavak, učenje i razvoj te komunikacija) utvrđene u ovoj Uredbi, financijski subjekti trebali bi se i dalje moći koristiti drukčije oblikovanim ili kategoriziranim modelima upravljanja IKT rizicima.

(48) Kako bi održali korak s novim kiberprijetnjama, financijski subjekti trebali bi održavati ažurirane i pouzdane sustave IKT-a koji su sposobni osigurati ne samo obradu podataka potrebnih za pružanje njihovih usluga, nego i dostatnu tehnološku otpornost da na odgovarajući način mogu odgovoriti na dodatne potrebe za obradom zbog stresnih okolnosti na tržištu ili drugih nepovoljnih situacija.

(49) Učinkoviti planovi kontinuiteta poslovanja i planovi oporavka potrebni su kako bi se financijskim subjektima omogućilo da odmah i brzo riješe IKT incidente, osobito kibernapade, ograničavanjem štete i davanjem prednosti nastavku obavljanja aktivnosti i mjerama oporavka u skladu s njihovim politikama za izradu sigurnosnih kopija. Međutim, takvim nastavkom ni na koji se način ne bi smjela ugroziti cjelovitost i sigurnost mrežnih i informacijskih sustava ili dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka.

(50) Iako se ovom Uredbom financijskim subjektima daje fleksibilnost pri utvrđivanju njihovih ciljeva u pogledu vremena i točke oporavka i, posljedično, da utvrde te ciljeve vodeći u punoj mjeri računa o prirodi i ključnosti relevantnih funkcija i svim specifičnim poslovnim potrebama, njome bi se ipak trebala propisati obveza financijskih subjekata da pri utvrđivanju takvih ciljeva provedu procjenu mogućeg sveukupnog učinka na učinkovitost tržišta.

(51) Širitelji kibernapada obično nastoje ostvariti financijsku dobit izravno na izvoru, čime financijske subjekte izlažu znatnim posljedicama. Kako bi se spriječio gubitak cjelovitosti sustava IKT-a ili kako bi se spriječila njihova nedostupnost, a time i izbjegle povrede podataka i šteta na fizičkoj infrastrukturi IKT-a, trebalo bi znatno poboljšati i racionalizirati izvješćivanje financijskih subjekata o velikim IKT incidentima. Izvješćivanje o IKT incidentima trebalo bi uskladiti uvođenjem zahtjeva za sve financijske subjekte da izravno izvješćuju svoja relevantna nadležna tijela. Ako financijski subjekt podliježe nadzoru više nacionalnih nadležnih tijela, države članice trebale bi imenovati jedinstveno nadležno tijelo kao adresata takvog izvješćivanja. Kreditne institucije klasificirane kao značajne u skladu s člankom 6. stavkom 4. Uredbe Vijeća (EU) br. 1024/2013 ([19]) trebale bi podnijeti takvo izvješće nacionalnim nadležnim tijelima, koja bi izvješće naknadno trebala proslijediti Europskoj središnjoj banci (ESB).

(52) Izravno izvješćivanje trebalo bi omogućiti financijskim nadzornim tijelima izravan pristup informacijama o značajnim IKT incidentima. Financijska nadzorna tijela trebala bi pak prosljeđivati pojedinosti o značajnim IKT incidentima javnim nefinancijskim tijelima (kao što su nadležna tijela i jedinstvene kontaktne točke iz Direktive (EU) 2022/2555, nacionalna tijela za zaštitu podataka i tijela za izvršavanje zakonodavstva za značajne IKT incidente kaznene prirode) kako bi se povećala svijest takvih tijela o takvim incidentima i, u slučaju CSIRT-ova, olakšala brza pomoć koja se, prema potrebi, može pružiti financijskim subjektima. Uz navedeno, države članice trebale bi moći utvrditi da bi sami financijski subjekti trebali pružiti takve informacije tijelima javne vlasti izvan područja financijskih usluga. Tim bi se tokovima informacija trebalo omogućiti financijskim subjektima da brzo iskoriste sve relevantne tehničke doprinose, savjete o korektivnim mjerama i naknadno praćenje koje osiguravaju takva tijela. Informacije o značajnim IKT incidentima trebale bi teći u oba smjera: financijska nadzorna tijela trebala bi financijskim subjektima dostaviti sve potrebne povratne informacije ili smjernice, dok bi europska nadzorna tijela trebala dijeliti anonimizirane podatke o kiberprijetnjama i ranjivostima povezanima s određenim incidentom kako bi doprinijela široj zajedničkoj obrani.

(53) Iako bi svi financijski subjekti trebali biti obvezni izvješćivati o incidentima, taj zahtjev ne bi na njih sve trebao utjecati na isti način. Stoga bi relevantne pragove značajnosti, kao i rokove izvješćivanja, trebalo na odgovarajući način prilagoditi, u kontekstu delegiranih akata koji se temelje na regulatornim tehničkim standardima koje trebaju razviti europska nadzorna tijela, kako bi se obuhvatili samo značajni IKT incidenti. Uz navedeno, pri određivanju rokova za obveze izvješćivanja trebalo bi uzeti u obzir posebnosti financijskih subjekata.

(54) Ovom bi se Uredbom od kreditnih institucija, institucija za platni promet, pružatelja usluga pružanja informacija o računu i institucija za elektronički novac trebalo zahtijevati da izvješćuju o svim operativnim ili sigurnosnim incidentima povezanima s plaćanjem, o kojima se prethodno izvješćivalo na temelju Direktive (EU) 2015/2366, neovisno o IKT aspektu incidenta.

([19]) 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.).

(55) Europska nadzorna tijela trebala bi imati zadaću procjene izvedivosti i uvjeta za moguću centralizaciju izvješćâ o IKT incidentima na razini Unije. Takva centralizacija mogla bi se sastojati od jedinstvenog EU-ova centra za izvješćivanje o značajnim IKT incidentima koji izravno prima relevantna izvješća i automatski obavješćuje nacionalna nadležna tijela, ili samo centralizira relevantna izvješća koja dostavljaju nacionalna nadležna tijela i time ispunjava koordinacijsku ulogu. Europska nadzorna tijela trebala bi imati zadaću pripreme, uz savjetovanje s ESB-om i ENISA-om, zajedničkog izvješća u kojem se razmatra izvedivost uspostave jedinstvenog EU-ova centra.

(56) Kako bi postigli visoku razinu digitalne operativne otpornosti te u skladu i s relevantnim međunarodnim standardima (npr. dokument skupine G-7 „Fundamental Elements for Threat-Led Penetration Testing" (Temeljni elementi za penetracijska testiranja vođena prijetnjama)) i s okvirima koji se primjenjuju u Uniji, kao što je TIBER-EU, financijski subjekti trebali bi redovito testirati svoje sustave IKT-a i osoblje koje ima odgovornosti u pogledu IKT-a s obzirom na djelotvornost njihovih sposobnosti za sprečavanje, otkrivanje, odgovor i oporavak radi otkrivanja i uklanjanja mogućih ranjivosti u području IKT-a. Kako bi se odrazile razlike koje postoje u pogledu razine pripravnosti financijskih subjekata u području kibersigurnosti među različitim financijskim podsektorima, i unutar njih, testiranje bi trebalo uključivati širok raspon alata i mjera, koji se proteže od procjene osnovnih zahtjeva (npr. procjene i skeniranja ranjivosti, analize javno dostupnih izvora, procjene mrežne sigurnosti, analize odstupanja, preispitivanja fizičke sigurnosti, upitnici i softverska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvedivo, testiranja na temelju scenarija, testiranja kompatibilnosti, testiranja performansi ili integralno testiranje) do naprednijeg testiranja na temelju penetracijskog testiranja vođenog prijetnjama (TLPT). Takvo napredno testiranje trebalo bi zahtijevati samo od financijskih subjekata koji su iz perspektive IKT-a dostatno zreli da ga u razumnoj mjeri mogu provesti. Testiranje digitalne operativne otpornosti koje se zahtijeva ovom Uredbom trebalo bi tako biti zahtjevnije za one financijske subjekte koji ispunjavaju kriterije utvrđene u ovoj Uredbi (na primjer kreditne institucije koje su velike, sistemski značajne i zrele kad je riječ o IKT-u, burze, središnji depozitoriji vrijednosnih papira i središnje druge ugovorne strane) nego za druge financijske subjekte. Istodobno bi testiranje digitalne operativne otpornosti na temelju TLPT-a trebalo biti relevantnije za financijske subjekte koji posluju u podsektorima ključnih financijskih usluga i imaju sistemsku ulogu (na primjer plaćanja, bankarstvo te kliring i namira), a manje relevantno za druge podsektore (na primjer upravitelji imovine i agencije za kreditni rejting).

(57) Financijski subjekti koji su uključeni u prekogranične aktivnosti i ostvaruju slobodu poslovnog nastana, ili slobodu pružanja usluga u Uniji, trebali bi ispunjavati jedinstvene zahtjeve naprednog testiranja (npr. TLPT) u svojoj matičnoj državi članici, koje bi trebalo uključivati infrastrukture IKT-a u svim jurisdikcijama u kojima prekogranična financijska grupa posluje u Uniji, čime bi se takvim prekograničnim financijskim grupama omogućilo da troškove testiranja povezane s IKT-om snose samo u jednoj jurisdikciji.

(58) Kako bi se iskoristilo stručno znanje koje su stekla određena nadležna tijela, osobito u pogledu provedbe okvira TIBER–EU, ovom bi se Uredbom državama članicama trebalo omogućiti da imenuju jedinstveno tijelo javne vlasti koje je na nacionalnoj razini u financijskom sektoru odgovorno za sva pitanja povezana s TLPT-om, ili nadležna tijela, koja, u slučaju da takvo imenovanje nije provedeno, delegiraju izvršavanje zadaća povezanih s TLPT-om drugom nacionalnom financijskom nadležnom tijelu.

(59) Budući da se ovom Uredbom od financijskih subjekata ne zahtijeva da sve ključne ili važne funkcije obuhvate jedinstvenim penetracijskim testom vođenim prijetnjama, financijski subjekti trebali bi moći slobodno odrediti koje bi i koliko ključnih ili važnih funkcija trebalo obuhvatiti takvim testom.

(60) Skupno testiranje u smislu ove Uredbe, koje uključuje sudjelovanje nekoliko financijskih subjekata u TLPT-u i za koje treća strana pružatelj IKT usluga može izravno sklopiti ugovorne aranžmane s vanjskim provoditeljem testiranja, trebalo bi biti dopušteno samo ako se očekuje negativan utjecaj na kvalitetu ili sigurnost usluga koje treća strana pružatelj IKT usluga pruža klijentima koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe ili povjerljivost podataka povezanih s takvim uslugama. Skupno testiranje trebalo bi podlijegati i zaštitnim mjerama (pod vodstvom jednog imenovanog financijskog subjekta i uz utvrđivanje broja financijskih subjekata sudionika) kako bi se osigurao rigorozan postupak testiranja za uključene financijske subjekte koji ispunjavaju ciljeve TLPT-a na temelju ove Uredbe.

(61) Kako bi se iskoristili unutarnji resursi dostupni na korporativnoj razini, ovom bi se Uredbom trebala omogućiti upotreba unutarnjih provoditelja testiranja za potrebe provedbe TLPT-a, pod uvjetom da postoji odobrenje nadzornih tijela, da nema sukoba interesa i da se provode periodične izmjene upotrebe unutarnjih i vanjskih provoditelja testiranja (svaka tri testa), pri čemu se zahtijeva da pružatelj saznanja o prijetnjama u TLPT-u nikad ne smije biti dio financijskog subjekta. Financijski subjekt trebao bi u punoj mjeri ostati odgovoran za provedbu TLPT-a. Potvrde koje izdaju tijela trebale bi služiti isključivo u svrhu uzajamnog priznavanja te se njima ne bi smjelo isključivati eventualne daljnje mjere potrebne za nošenje s IKT rizikom kojem je financijski subjekt izložen niti bi ih trebalo smatrati odobrenjem nadzornih tijela u pogledu sposobnosti financijskog subjekta za upravljanje IKT rizicima i njihovo ublažavanje.

(62) Kako bi se u financijskom sektoru osiguralo pouzdano praćenje IKT rizika povezanog s trećim stranama, potrebno je utvrditi skup pravila utemeljenih na načelima radi pružanja smjernica financijskim subjektima pri praćenju rizika koji nastaje u kontekstu funkcija eksternaliziranih trećim stranama pružateljima IKT usluga, osobito za IKT usluge kojima se podupiru ključne ili važne funkcije, kao i općenitije u kontekstu svih ovisnosti o trećim stranama u području IKT-a.

(63) Kako bi se uvažila složenost različitih izvora IKT rizika, uzimajući u obzir brojnost i raznolikost pružatelja tehnoloških rješenja koja omogućuju neometano pružanje financijskih usluga, ovom bi Uredbom trebalo obuhvatiti širok raspon trećih strana pružatelja IKT usluga, uključujući pružatelje usluga računalstva u oblaku, softvera, usluga analize podataka i pružatelje usluga podatkovnog centra. Slično tome, budući da bi financijski subjekti trebali djelotvorno i dosljedno utvrđivati sve vrste rizika i upravljati njima, među ostalim i u kontekstu IKT usluga nabavljenih unutar financijske grupe, trebalo bi pojasniti da bi se društva koja su dio financijske grupe te pružaju IKT usluge uglavnom svojem matičnom društvu ili društvima kćerima ili podružnicama svojeg matičnog društva, kao i financijski subjekti koji pružaju IKT usluge drugim financijskim subjektima, također trebala smatrati pružateljima IKT usluga na temelju ove Uredbe. Naposljetku, s obzirom na to da evoluirajuće tržište platnih usluga postaje sve ovisnije o složenim tehničkim rješenjima te s obzirom na nove vrste platnih usluga i rješenja povezanih s plaćanjem, sudionike u ekosustavu platnih usluga, koji osiguravaju aktivnosti obrade plaćanja ili upravljaju infrastrukturama platnog prometa, također bi trebalo smatrati trećim stranama pružateljima IKT usluga na temelju ove Uredbe, uz iznimku središnjih banaka kad upravljaju platnim sustavima ili sustavima namire vrijednosnih papira te tijela javne vlasti kad pružaju IKT usluge u kontekstu izvršavanja državnih funkcija.

(64) Financijski subjekt trebao bi u svakom trenutku ostati potpuno odgovoran za ispunjenje svojih obveza utvrđenih u ovoj Uredbi. Financijski subjekti trebali bi primijeniti proporcionalan pristup praćenju rizika koji se javljaju na razini trećih strana pružatelja IKT usluga, vodeći računa o prirodi, opsegu, složenosti i važnosti svojih ovisnosti u području IKT-a, ključnosti ili važnosti usluga, procesa ili funkcija koje podliježu ugovornim aranžmanima i, u konačnici, na temelju detaljne procjene mogućeg učinka na kontinuitet i kvalitetu financijskih usluga na pojedinačnoj razini i na razini grupe, ovisno o slučaju.

(65) Provedba takvog praćenja trebala bi se odvijati u skladu sa strateškim pristupom IKT riziku povezanom s trećim stranama koji je upravljačko tijelo financijskog subjekta formaliziralo donošenjem namjenske strategije o IKT riziku povezanom s trećim stranama, a koja se temelji na kontinuiranoj dubinskoj analizi svih ovisnosti o trećim stranama u području IKT-a. Kako bi se unaprijedila razina osviještenosti nadzornih tijela o ovisnostima o trećim stranama u području IKT-a te dodatno podupro rad u kontekstu nadzornog okvira uspostavljenog ovom Uredbom, trebalo bi zahtijevati od svih financijskih subjekata da vode registar informacija o svim ugovornim aranžmanima za upotrebu IKT usluga koje pružaju treće strane pružatelji IKT usluga. Financijska nadzorna tijela trebala bi moći zatražiti cijeli registar ili određene dijelove tog registra te tako dobiti ključne informacije za stjecanje šireg razumijevanja ovisnosti koje financijski subjekti imaju u području IKT-a.

(66) Formalno sklapanje ugovornih aranžmana trebalo bi se temeljiti na detaljnoj prethodnoj predugovornoj analizi, osobito usmjeravanjem na elemente kao što su ključnost ili važnost usluga koje se podupiru predviđenim ugovorom o IKT-u, potrebna odobrenja nadzornih tijela ili drugi uvjeti, mogući povezani koncentracijski rizik, te primjenom dubinske analize u postupku odabira i procjene trećih strana pružatelja IKT usluga i procjenom potencijalnih sukoba interesa. Kad je riječ o ugovornim aranžmanima koji se odnose na ključne ili važne funkcije, financijski subjekti trebali bi razmotriti upotrebljavaju li treće strane pružatelji IKT usluga najnovije i najviše

standarde informacijske sigurnosti. Raskid ugovornih aranžmana mogao bi nastupiti barem zbog niza okolnosti koje ukazuju na nedostatke na razini treće strane pružatelja IKT usluga, osobito u smislu znatnih kršenja zakona ili ugovornih uvjeta, okolnosti koje ukazuju na moguću promjenu u obavljanju funkcija predviđenih u ugovornim aranžmanima, dokaza o slabostima treće strane pružatelja IKT usluga u općem upravljanju IKT rizicima, ili okolnosti koje upućuju na nemogućnost relevantnog nadležnog tijela da djelotvorno nadzire financijski subjekt.

(67) Kako bi se ublažio sistemski učinak koncentracijskog IKT rizika povezanog s trećim stranama, ovom se Uredbom promiče uravnoteženo rješenje primjenom fleksibilnog i postupnog pristupa takvom koncentracijskom riziku jer bi nametanje bilo kakvih strogih gornjih vrijednosti ili strogih ograničenja moglo ometati poslovanje i ograničiti ugovornu slobodu. Financijski subjekti trebali bi temeljito procijeniti svoje predviđene ugovorne aranžmane kako bi utvrdili vjerojatnost pojave takvog rizika, među ostalim i s pomoću dubinskih analiza podugovornih aranžmana, osobito kad se sklapaju s trećim stranama pružateljima IKT usluga s poslovnim nastanom u trećoj zemlji. U toj fazi i u cilju postizanja pravedne ravnoteže između nužnog očuvanja ugovorne slobode i jamčenja financijske stabilnosti smatra se da nije primjereno utvrditi pravila o strogim gornjim vrijednostima i ograničenja za izloženosti trećim stranama u području IKT-a. U kontekstu nadzornog okvira glavno nadzorno tijelo imenovano na temelju ove Uredbe trebalo bi, u pogledu ključnih trećih strana pružatelja IKT usluga, posebnu pozornost posvetiti potpunom razumijevanju razmjera međuovisnosti, otkriti konkretne slučajeve u kojima je vjerojatno da će visok stupanj koncentracije ključnih trećih strana pružatelja IKT usluga opteretiti stabilnost i cjelovitost financijskog sustava Unije te održavati dijalog s ključnim trećim stranama pružateljima IKT usluga kad se taj konkretan rizik utvrdi.

(68) Kako bi se redovito evaluirala i pratila sposobnost treće strane pružatelja IKT usluga da sigurno pruža usluge financijskom subjektu bez negativnih učinaka na digitalnu operativnu otpornost financijskog subjekta, trebalo bi uskladiti nekoliko ključnih ugovornih elemenata s trećim stranama pružateljima IKT usluga. Takvim usklađivanjem trebalo bi obuhvatiti minimalna područja koja su ključna kako bi se financijskom subjektu omogućilo potpuno praćenje rizika koji bi mogli nastati od treće strane pružatelja IKT usluga, iz perspektive potrebe financijskog subjekta da osigura svoju digitalnu otpornost jer uvelike ovisi o stabilnosti, funkcionalnosti, dostupnosti i sigurnosti IKT usluga koje prima.

(69) Pri ponovnom pregovaranju o ugovornim aranžmanima radi usklađivanja sa zahtjevima iz ove Uredbe, financijski subjekti i treće strane pružatelji IKT usluga trebali bi osigurati da budu obuhvaćene ključne ugovorne odredbe kako je predviđeno u ovoj Uredbi.

(70) Definicija „ključne ili važne funkcije” predviđena u ovoj Uredbi obuhvaća „ključne funkcije” kako su definirane u članku 2. stavku 1. točki 35. Direktive 2014/59/EU Europskog parlamenta i Vijeća ([20]). U skladu s tim, funkcije koje se smatraju ključnima na temelju Direktive 2014/59/EU uključene su u definiciju ključnih funkcija u smislu ove Uredbe.

(71) Neovisno o ključnosti ili važnosti funkcije koja se podupire IKT uslugama, ugovornim aranžmanima posebno bi trebalo predvidjeti specifikaciju potpunih opisa funkcija i usluga, lokacija na kojima se takve funkcije pružaju i na kojima treba obrađivati podatke, kao i navođenje opisa razina usluge. Drugi ključni elementi za omogućavanje financijskom subjektu da prati IKT rizik povezan s trećim stranama su: ugovorne odredbe kojima se propisuje način na koji treća strana pružatelj IKT usluga treba osigurati pristupačnost, dostupnost, cjelovitost, sigurnost i zaštitu osobnih podataka; odredbe kojima se utvrđuju relevantna jamstva za omogućivanje pristupa, oporavka i povrata podataka u slučaju nesolventnosti, sanacije ili prekida poslovanja treće strane pružatelja IKT usluga, kao i odredbe kojima se od treće strane pružatelja IKT usluga zahtijeva da pruži pomoć u slučaju IKT incidenata povezanih s

([20]) Direktiva 2014/59/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o uspostavi okvira za oporavak i sanaciju kreditnih institucija i investicijskih društava te o izmjeni Direktive Vijeća 82/891/EEZ i direktiva 2001/24/EZ, 2002/47/EZ, 2004/25/EZ, 2005/56/EZ, 2007/36/EZ, 2011/35/EU, 2012/30/EU i 2013/36/EU te uredbi (EU) br. 1093/2010 i (EU) br. 648/2012 Europskog parlamenta i Vijeća (SL L 173, 12.6.2014., str. 190.).

pruženim uslugama, bez dodatnih troškova ili uz ex ante utvrđene troškove; odredbe o obvezi treće strane pružatelja IKT usluga da u potpunosti surađuje s nadležnim i sanacijskim tijelima zaduženima za financijski subjekt; i odredbe o pravima raskida i povezanim minimalnim rokovima za prethodnu obavijest u vezi s raskidom ugovornih aranžmana, u skladu s očekivanjima nadležnih tijela i sanacijskih tijela.

(72) Uz takve ugovorne odredbe i kako bi se osiguralo da financijski subjekti zadrže potpunu kontrolu nad svim događajima na razini trećih strana koji bi mogli narušiti njihovu sigurnost u području IKT-a, ugovorima o pružanju IKT usluga kojima se podupiru ključne ili važne funkcije trebalo bi predvidjeti i sljedeće: specifikaciju cjelovitih opisa razina usluge, s preciznim kvantitativnim i kvalitativnim ciljevima uspješnosti, kako bi se bez nepotrebne odgode omogućile odgovarajuće korektivne mjere kad dogovorene razine usluge nisu ispunjene; relevantne rokove za prethodne obavijesti i obveze izvješćivanja koje ima treća strana pružatelj IKT usluga u slučaju razvoja događaja koji bi mogli bitno utjecati na sposobnost treće strane pružatelja IKT usluga da učinkovito pruža svoje dotične IKT usluge; zahtjev da treća strana pružatelj IKT usluga provede i testira planove za nepredvidive situacije u poslovanju i da ima sigurnosne mjere, alate i politike u području IKT-a kojima se omogućuje sigurno pružanje usluga te da sudjeluje i u potpunosti surađuje u TLPT-u koji provodi financijski subjekt.

(73) Takvi ugovori o pružanju IKT usluga kojima se podupiru ključne ili važne funkcije trebali bi također sadržavati odredbe kojima se financijskom subjektu ili imenovanoj trećoj strani omogućuje pravo pristupa, pravo inspekcijskog nadzora i pravo revizije te pravo na izradu kopija kao ključnih instrumenata u okviru kontinuiranog praćenja rada treće strane pružatelja IKT usluga od strane financijskih subjekata, kao i potpuna suradnja pružatelja usluga tijekom inspekcijskog nadzora. Slično tome, nadležno tijelo zaduženo za financijski subjekt trebalo bi, na temelju prethodnih obavijesti, imati prava inspekcijskog nadzora i revizije treće strane pružatelja IKT usluga, uz uvažavanje zaštite povjerljivih informacija.

(74) Takvim ugovornim aranžmanima trebale bi se predvidjeti i namjenske izlazne strategije kako bi se osobito omogućila obvezna prijelazna razdoblja tijekom kojih bi treće strane pružatelji IKT usluga trebale nastaviti pružati relevantne usluge u cilju smanjenja rizika od poremećaja na razini financijskog subjekta ili kako bi se tom subjektu omogućilo da se djelotvorno započne koristiti uslugama nekih drugih trećih strana pružatelja IKT usluga ili da se, alternativno, prebaci na interna rješenja, ovisno o složenosti pružene IKT usluge. Nadalje, financijski subjekti obuhvaćeni područjem primjene Direktive 2014/59/EU trebali bi osigurati da relevantni ugovori o IKT uslugama budu pouzdani i u potpunosti izvršivi u slučaju sanacije tih financijskih subjekata. Stoga bi, u skladu s očekivanjima sanacijskih tijela, ti financijski subjekti trebali osigurati otpornost relevantnih ugovora o IKT uslugama u slučaju sanacije. Dok god i dalje ispunjavaju svoje obveze u pogledu plaćanja, ti bi financijski subjekti, uz ostale zahtjeve, trebali osigurati da relevantni ugovori za IKT usluge sadržavaju odredbe prema kojima se ne mogu raskinuti, suspendirati niti izmijeniti zbog restrukturiranja ili sanacije.

(75) Nadalje, dobrovoljnom primjenom standardnih ugovornih klauzula koje su razvila tijela javne vlasti ili institucije Unije, posebno upotrebom ugovornih klauzula koje je Komisija razvila za usluge računalstva u oblaku, moglo bi se dodatno ojačati povjerenje financijskih subjekata i trećih strana pružatelja IKT usluga jer bi se povećao stupanj pravne sigurnosti u pogledu upotrebe usluga računalstva u oblaku u financijskom sektoru, što je u potpunosti u skladu sa zahtjevima i očekivanjima utvrđenima pravom Unije o financijskim uslugama. Razvoj standardnih ugovornih klauzula temelji se na mjerama koje su već predviđene Akcijskim planom za financijske tehnologije (2018.) u kojem je najavljeno da Komisija namjerava poticati i olakšati izradu standardnih ugovornih odredbi za financijske subjekte koji eksternaliziraju poslove pružateljima usluga računalstva u oblaku, oslanjajući se pritom na međusektorske napore dionika u području usluga računalstva u oblaku, uz posredovanje Komisije i sudjelovanje financijskog sektora.

(76) Ključne treće strane pružatelje IKT usluga trebalo bi obuhvatiti nadzornim okvirom Unije kako bi se promicali konvergencija i učinkovitost u pogledu pristupa nadzornih tijela u nošenju s IKT rizikom povezanim s trećim stranama u financijskom sektoru te jačala digitalna operativna otpornost financijskih subjekata koji se za IKT usluge kojima se podupire pružanje financijskih usluga oslanjaju na ključne treće strane pružatelje IKT usluga i kako bi se time doprinijelo očuvanju stabilnosti financijskog sustava Unije i cjelovitosti unutarnjeg tržišta za financijske usluge.

Iako opravdanost uspostave nadzornog okvira proizlazi iz dodane vrijednosti poduzimanja mjera na razini Unije i suštinske uloge i posebnosti upotrebe IKT usluga u pružanju financijskih usluga, istodobno bi trebalo podsjetiti da se to rješenje čini prikladnim samo u kontekstu ove Uredbe koja se konkretno odnosi na digitalnu operativnu otpornost u financijskom sektoru. Međutim, takav nadzorni okvir ne bi se trebao smatrati novim modelom nadzora na razini Unije u drugim područjima financijskih usluga i aktivnosti.

(77) Nadzorni okvir trebao bi se primjenjivati samo na ključne treće strane pružatelje IKT usluga. Stoga bi trebao postojati mehanizam imenovanja kako bi se u obzir uzeli dimenzija i priroda oslanjanja financijskog sektora na takve treće strane pružatelje IKT usluga. Taj mehanizam trebao bi obuhvaćati skup kvantitativnih i kvalitativnih kriterija za utvrđivanje parametara ključnosti kao osnove za uključivanje u nadzorni okvir. Kako bi se osigurala točnost te procjene i neovisno o korporativnoj strukturi treće strane pružatelja IKT usluga, takvim bi se kriterijima, u slučaju treće strane pružatelja IKT usluga koja je dio šire grupe, trebala uzeti u obzir cjelokupna struktura grupe u kojoj je treća strana pružatelja IKT usluga. S jedne strane, ključne treće strane pružatelji IKT usluga koje nisu automatski određene na temelju primjene tih kriterija trebale bi imati mogućnost dobrovoljnog sudjelovanja u nadzornom okviru, dok bi, s druge strane, treće strane pružatelji IKT usluga koje već podliježu okvirima nadzornog mehanizma kojima se podupire ispunjavanje zadaća Europskog sustava središnjih banaka, kako je navedeno u članku 127. stavku 2. UFEU-a, trebale biti izuzete.

(78) Slično tome, financijski subjekti koji pružaju IKT usluge drugim financijskim subjektima, iako pripadaju kategoriji trećih strana pružatelja IKT usluga na temelju ove Uredbe, također bi trebali biti izuzeti iz nadzornog okvira jer već podliježu nadzornim mehanizmima uspostavljenima relevantnim pravom Unije o financijskim uslugama. Ako je to primjenjivo, nadležna tijela trebala bi u kontekstu svojih nadzornih aktivnosti uzeti u obzir IKT rizik koji financijski subjekti koji pružaju IKT usluge predstavljaju za financijske subjekte. Isto tako, zbog postojećih mehanizama za praćenje rizika na razini grupe isto bi izuzeće trebalo uvesti za treće strane pružatelje IKT usluga koji uglavnom pružaju usluge subjektima iz svoje grupe. Treće strane pružatelji IKT usluga koje IKT usluge pružaju isključivo u jednoj državi članici financijskim subjektima koji posluju samo u toj državi članici također bi zbog svojih ograničenih aktivnosti i izostanka prekograničnog učinka trebali biti izuzeti od mehanizma imenovanja.

(79) Digitalna transformacija u području financijskih usluga dovela je do nezapamćenih razmjera upotrebe IKT usluga i oslanjanja na njih. Budući da je pružanje financijskih usluga bez upotrebe usluga računalstva u oblaku, softverskih rješenja i usluga povezanih s podacima postalo nezamislivo, financijski ekosustav Unije postao je suštinski ovisan o određenim IKT uslugama koje pružaju pružatelji IKT usluga. Neki od tih pružatelja inovatori su u razvoju i primjeni tehnologija temeljenih na IKT-u i imaju važnu ulogu u pružanju financijskih usluga ili su se integrirali u vrijednosni lanac financijskih usluga. Time su postali ključni za stabilnost i cjelovitost financijskog sustava Unije. To široko oslanjanje na usluge koje pružaju ključne treće strane pružatelji IKT usluga, u kombinaciji s međuovisnošću informacijskih sustava različitih tržišnih subjekata, stvara izravan i potencijalno ozbiljan rizik za sustav financijskih usluga Unije i kontinuitet pružanja financijskih usluga ako na ključne treće strane pružatelje IKT usluga utječu operativni poremećaji ili značajni kiberincidenti. Kiberincidenti se u financijskom sustavu mogu umnožavati i širiti znatno brže od drugih vrsta rizika koji se prate u financijskom sektoru te se mogu proširiti među sektorima i preko zemljopisnih granica. Mogu prerasti u sistemsku krizu koja narušava povjerenje u financijski sustav zbog poremećaja u funkcijama kojima se podupire realno gospodarstvo ili zbog znatnih financijskih gubitaka na razini koju financijski sustav ne može podnijeti ili koja zahtijeva uvođenje mjera za ublažavanje teških šokova. Kako bi se spriječilo ostvarivanje tih scenarija i ugrožavanje financijske stabilnosti i cjelovitosti Unije, izuzetno je važno osigurati konvergenciju nadzornih praksi u vezi s IKT rizikom povezanim s trećim stranama u području financija, osobito s pomoću novih pravila kojima se omogućuje nadzor Unije nad ključnim trećim stranama pružateljima IKT usluga.

(80) Nadzorni okvir uvelike ovisi o stupnju suradnje između glavnog nadzornog tijela i ključne treće strane pružatelja IKT usluga koja financijskim subjektima pruža usluge koje utječu na pružanje financijskih usluga. Uspješan nadzor temelji se, među ostalim, na sposobnosti glavnog nadzornog tijela da djelotvorno provodi misije praćenja i inspekcijski nadzor radi procjene pravila, kontrola i procesa koje upotrebljavaju ključne treće strane pružatelji IKT usluga te radi procjene mogućeg kumulativnog učinka njihovih aktivnosti na financijsku stabilnost i cjelovitost financijskog sustava. Istodobno je od presudne važnosti da ključne treće strane pružatelji IKT usluga slijede preporuke glavnog nadzornog tijela i otklone njegove bojazni. Budući da bi izostanak suradnje ključne treće strane pružatelja IKT usluga koja pruža usluge koje utječu na pružanje financijskih usluga, kao što je odbijanje davanja pristupa njezinim prostorima ili odbijanje pružanja informacija, u konačnici lišio glavno nadzorno tijelo njegovih ključnih alata za procjenu IKT rizika povezanog s trećim stranama te bi mogao negativno utjecati na financijsku stabilnost i cjelovitost financijskog sustava, potrebno je predvidjeti i razmjeran sustav sankcija.

(81) U tom kontekstu, potreba glavnog nadzornog tijela da izrekne novčane kazne kako bi ključne treće strane pružatelje IKT usluga primoralo na poštovanje obveza u pogledu transparentnosti i pristupa utvrđenih u ovoj Uredbi ne bi trebala biti ugrožena zbog poteškoća koje proizlaze iz izvršenja tih novčanih kazni u odnosu na ključne treće strane pružatelje IKT usluga s poslovnim nastanom u trećim zemljama. Kako bi se osigurala izvršivost takvih kazni i omogućilo brzo uvođenje postupaka za očuvanje pravâ ključnih trećih strana pružatelja IKT usluga na obranu u kontekstu mehanizma imenovanja te izdavanja preporuka, od tih ključnih trećih strana pružatelja IKT usluga, koje financijskim subjektima pružaju usluge koje utječu na pružanje financijskih usluga, trebalo bi zahtijevati da održavaju odgovarajuću poslovnu prisutnost u Uniji. Zbog prirode nadzora i nepostojanja usporedivih aranžmana u drugim jurisdikcijama ne postoje prikladni alternativni mehanizmi kojima bi se taj cilj osigurao djelotvornom suradnjom s financijskim nadzornim tijelima u trećim zemljama u pogledu praćenja učinka digitalnih operativnih rizika koje predstavljaju sistemske treće strane pružatelji IKT usluga koje se smatraju ključnim trećim stranama pružateljima IKT usluga s poslovnim nastanom u trećim zemljama. Kako bi stoga nastavila pružati IKT usluge financijskim subjektima u Uniji, treća strana pružatelj IKT usluga s poslovnim nastanom u trećoj zemlji koja je imenovana kao ključna u skladu s ovom Uredbom trebala bi u roku od 12 mjeseci od takvog imenovanja poduzeti sve potrebne mjere kako bi osigurala da je osnovana u Uniji, i to tako da uspostavi društvo kći, kako je definirano u pravnoj stečevini Unije, odnosno u Direktivi 2013/34/EU Europskog parlamenta i Vijeća ([21]).

(82) Zahtjev da osnuje društvo kći u Uniji ne bi trebao spriječiti ključnu treću stranu pružatelja IKT usluga da pruža IKT usluge i povezanu tehničku potporu iz objekata i infrastrukture koji se nalaze izvan Unije. Ovom se Uredbom ne bi trebala nametati obveza u pogledu lokalizacije podataka jer se njome ne zahtijeva pohrana ili obrada podataka u Uniji.

(83) Ključne treće strane pružatelji IKT usluga trebale bi moći pružati IKT usluge iz bilo kojeg dijela svijeta, ne nužno ili ne samo iz prostora koji se nalaze u Uniji. Aktivnosti nadzora prvo bi se trebale provoditi u prostorima koji se nalaze u Uniji i interakcijom sa subjektima koji se nalaze u Uniji, uključujući društva kćeri koja su osnovale ključne treće strane pružatelji IKT usluga na temelju ove Uredbe. Međutim, takva djelovanja unutar Unije mogla bi biti nedostatna da bi se glavnom nadzornom tijelu omogućilo da u potpunosti i djelotvorno obavlja svoje zadaće na temelju ove Uredbe. Glavno nadzorno tijelo stoga bi također trebalo moći izvršavati svoje relevantne nadzorne ovlasti u trećim zemljama. Izvršavanje tih ovlasti u trećim zemljama trebalo bi omogućiti glavnom nadzornom tijelu da ispita objekte iz kojih ključna treća strana pružatelj IKT usluga pruža IKT usluge ili usluge tehničke podrške, odnosno takvim uslugama upravlja, te bi glavnom nadzornom tijelu trebalo omogućiti sveobuhvatno i operativno razumijevanje upravljanja IKT rizicima koje provodi ključna treća strana pružatelj IKT usluga. Mogućnost da glavno nadzorno tijelo, kao agencija Unije, izvršava ovlasti izvan područja Unije trebala bi biti propisno uređena relevantnim uvjetima, posebno privolom dotične ključne treće strane pružatelja IKT usluga. Slično tome, relevantna tijela treće zemlje trebala bi biti obaviještena o izvršavanju aktivnosti glavnog nadzornog tijela na njihovu državnom području te se takvom izvršavanju aktivnosti ne bi smjela usprotiviti. Međutim, kako bi se osigurala učinkovita provedba i ne dovodeći u pitanje odgovarajuće nadležnosti institucija Unije i država članica, takve se ovlasti također trebaju u potpunosti temeljiti na sklapanju aranžmana za administrativnu suradnju s relevantnim tijelima dotične

([21]) Direktiva 2013/34/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o godišnjim financijskim izvještajima, konsolidiranim financijskim izvještajima i povezanim izvješćima za određene vrste poduzeća, o izmjeni Direktive 2006/43/EZ Europskog parlamenta i Vijeća i o stavljanju izvan snage direktiva Vijeća 78/660/EEZ i 83/349/EEZ (SL L 182, 29.6.2013., str. 19.).

treće zemlje. Ovom bi se Uredbom stoga europskim nadzornim tijelima trebalo omogućiti sklapanje aranžmana za administrativnu suradnju s relevantnim tijelima trećih zemalja, čime se ne bi trebale stvarati nikakve druge pravne obveze u odnosu na Uniju i njezine države članice.

(84) Kako bi se olakšala komunikacija s glavnim nadzornim tijelom i osiguralo odgovarajuće zastupanje, ključne treće strane pružatelji IKT usluga koji su dio grupe trebali bi imenovati jednu pravnu osobu kao svoju koordinacijsku točku.

(85) Nadzornim okvirom ne bi se trebala dovoditi u pitanje nadležnost država članica da provode vlastite misije nadzora ili praćenja trećih strana pružatelja IKT usluga koje nisu imenovane kao ključne na temelju ove Uredbe, ali se smatraju važnima na nacionalnoj razini.

(86) Kako bi se iskoristila višeslojna institucionalna struktura u području financijskih usluga, Zajednički odbor europskih nadzornih tijela trebao bi nastaviti osiguravati opću međusektorsku koordinaciju u vezi sa svim pitanjima koja se odnose na IKT rizik, u skladu sa svojim zadaćama u području kibersigurnosti. Potporu bi mu trebao pružati novi pododbor („Nadzorni forum”) koji obavlja pripremne radnje kako za pojedinačne odluke upućene ključnim trećim stranama pružateljima IKT usluga tako i za izdavanje zajedničkih preporuka, osobito u odnosu na usporednu analizu programâ nadzora ključnih trećih strana pružatelja IKT usluga i utvrđivanje najboljih praksi za rješavanje pitanjâ koncentracijskog IKT rizika.

(87) Kako bi se osigurao primjeren i djelotvoran nadzor nad ključnim trećim stranama pružateljima IKT usluga na razini Unije, ovom se Uredbom predviđa da bi se bilo koje od triju europskih nadzornih tijela moglo imenovati glavnim nadzornim tijelom. Pojedinačna dodjela ključne treće strane pružatelja IKT usluga jednom od triju europskih nadzornih tijela trebala bi biti rezultat procjene prevlasti financijskih subjekata koji posluju u financijskim sektorima za koje je to europsko nadzorno tijelo odgovorno. Taj bi pristup trebao dovesti do uravnotežene raspodjele zadaća i odgovornosti među trima europskim nadzornim tijelima u kontekstu izvršavanja nadzornih funkcija te bi se u okviru njega na najbolji način trebali iskoristiti ljudski resursi i tehničko stručno znanje kojim raspolaže svako od triju europskih nadzornih tijela.

(88) Glavnim nadzornim tijelima trebalo bi dodijeliti potrebne ovlasti za provedbu istraga, obavljanje izravnog i neizravnog inspekcijskog nadzora u prostorima i na lokacijama ključnih trećih strana pružatelja IKT usluga te za dobivanje potpunih i ažuriranih informacija. Tim bi se ovlastima glavnom nadzornom tijelu trebalo omogućiti da stekne stvaran uvid u vrstu, dimenziju i učinak IKT rizika povezanog s trećim stranama za financijske subjekte i, u konačnici, za financijski sustav Unije. Povjeravanje uloge glavnog nadzora europskim nadzornim tijelima preduvjet je za razumijevanje i rješavanje pitanja sistemske dimenzije IKT rizika u području financija. Učinak ključnih trećih strana pružatelja IKT usluga na financijski sektor Unije i mogući problemi uzrokovani povezanim koncentracijskim IKT rizikom iziskuju zajednički pristup na razini Unije. Istodobna provedba višestrukih revizija i prava pristupa, koje bi zasebno provodila brojna nadležna tijela uz malu ili nikakvu međusobnu koordinaciju, spriječila bi financijska nadzorna tijela da dobiju potpun i sveobuhvatan pregled IKT rizika povezanog s trećim stranama u Uniji te bi ujedno dovela do redundantnosti, opterećenja i složenosti za ključne treće strane pružatelje IKT usluga ako bi podlijegale brojnim zahtjevima u pogledu praćenja i inspekcijskog nadzora.

(89) Budući da imenovanje trećih strana pružatelja IKT usluga kao ključnih ima znatan učinak, ovom bi se Uredbom trebalo osigurati poštovanje prava ključnih trećih strana pružatelja IKT usluga tijekom provedbe cijelog nadzornog okvira. Prije nego što budu imenovani kao ključni, takvi bi pružatelji trebali, na primjer, imati pravo glavnom nadzornom tijelu dostaviti obrazloženu izjavu koja sadržava sve relevantne informacije u svrhu procjene povezane s njihovim imenovanjem. Budući da bi glavno nadzorno tijelo trebalo ovlastiti za podnošenje preporuka o pitanjima IKT rizika i odgovarajućim korektivnim mjerama, što uključuje ovlast za protivljenje određenim ugovornim aranžmanima koji u konačnici utječu na stabilnost financijskog subjekta ili financijskog sustava,

ključnim trećim stranama pružateljima IKT usluga trebalo bi omogućiti da prije finalizacije tih preporuka dostave objašnjenja o očekivanom učinku rješenja predviđenih u preporukama na klijente koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe te da osmisle rješenja za ublažavanje rizika. Ključne treće strane pružatelji IKT usluga koje se ne slažu s preporukama trebale bi dostaviti obrazloženo objašnjenje svoje namjere da ne prihvate preporuku. Ako se takvo obrazloženo objašnjenje ne dostavi ili se smatra nedostatnim, glavno nadzorno tijelo trebalo bi objaviti obavijest sa sažetim opisom neusklađenosti.

(90) Nadležna tijela trebala bi u svoje funkcije u pogledu bonitetnog nadzora financijskih subjekata propisno uključiti zadaću provjere sadržajne usklađenosti s preporukama koje je izdalo glavno nadzorno tijelo. Nadležna tijela trebala bi moći zahtijevati od financijskih subjekata da poduzmu dodatne mjere za nošenje s rizicima utvrđenima u preporukama glavnog nadzornog tijela te bi trebala pravodobno izdati obavijesti o tome. Ako glavno nadzorno tijelo uputi preporuke ključnim trećim stranama pružateljima IKT usluga koje su predmet nadzora na temelju Direktive (EU) 2022/2555, nadležna tijela trebala bi se moći, na dobrovoljnoj osnovi i prije donošenja dodatnih mjera, savjetovati s nadležnim tijelima iz te direktive kako bi se poticao koordiniran pristup u postupanju s dotičnim ključnim trećim stranama pružateljima IKT usluga.

(91) Izvršavanje nadzora trebalo bi se orijentirati prema trima operativnim načelima kojima se nastoji osigurati: (a) blisku koordinaciju među europskim nadzornim tijelima u njihovim ulogama glavnih nadzornih tijela putem Zajedničke nadzorne mreže, (b) usklađenost s okvirom uspostavljenim Direktivom (EU) 2022/2555 (na temelju dobrovoljnog savjetovanja s tijelima iz te direktive kako bi se izbjeglo udvostručavanje mjera usmjerenih na ključne treće strane pružatelje IKT usluga) i (c) dužnu pažnju u svrhu minimiziranja potencijalnog rizika od poremećaja u uslugama koje ključne treće strane pružatelji IKT usluga pružaju klijentima koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe.

(92) Nadzornim okvirom ne bi se trebao zamijeniti ni na bilo koji način ni u bilo kojem dijelu nadomjestiti zahtjev da financijski subjekti sami upravljaju rizicima koji proizlaze iz angažiranja trećih strana pružatelja IKT usluga, uključujući njihovu obvezu održavanja stalnog praćenja ugovornih aranžmana sklopljenih s ključnim trećim stranama pružateljima IKT usluga. Isto tako, nadzorni okvir ne bi trebao utjecati na potpunu odgovornost financijskih subjekata za poštovanje i izvršavanje svih pravnih obveza utvrđenih u ovoj Uredbi i u relevantnom pravu o financijskim uslugama.

(93) Kako bi se izbjegla udvostručavanja i preklapanja, nadležna tijela trebala bi se suzdržati od pojedinačnog poduzimanja bilo kakvih mjera usmjerenih na praćenje rizika ključne treće strane pružatelja IKT usluga te bi se u tom pogledu trebala oslanjati na procjenu relevantnog glavnog nadzornog tijela. O svim mjerama trebalo bi se svakako koordinirati i unaprijed ih dogovoriti s glavnim nadzornim tijelom u kontekstu izvršavanja zadaća iz nadzornog okvira.

(94) Kako bi se promicala konvergencija na međunarodnoj razini u pogledu primjene najboljih praksi u preispitivanju i praćenju upravljanja digitalnim rizicima trećih strana pružatelja IKT usluga, europska nadzorna tijela trebalo bi poticati na sklapanje aranžmana za suradnju s relevantnim nadzornim i regulatornim tijelima trećih zemalja.

(95) Kako bi se iskoristile posebne kompetencije, tehničke vještine i stručno znanje osoblja specijaliziranog za operativni i IKT rizik unutar nadležnih tijela, triju europskih nadzornih tijela te, na dobrovoljnoj osnovi, nadležnih tijela iz Direktive (EU) 2022/2555, glavno nadzorno tijelo trebalo bi se oslanjati na nacionalne nadzorne sposobnosti i znanje te osnovati namjenske timove za provjeru za svaku ključnu treću stranu pružatelja IKT usluga, udruživanjem multidisciplinarnih timova za potporu u pripremi i izvršenju nadzornih aktivnosti, uključujući opće istrage i inspekcijski nadzor nad ključnim trećim stranama pružateljima IKT usluga, kao i za sve potrebne daljnje mjere.

(96) Iako bi se troškovi koji proizlaze iz zadaća nadzora u potpunosti financirali naknadama koje se naplaćuju ključnim trećim stranama pružateljima IKT usluga, europskim nadzornim tijela vjerojatno će, prije početka primjene nadzornog okvira, nastati troškovi implementacije namjenskih IKT sustava na kojima će se temeljiti predstojeći nadzor, s obzirom na činjenicu da bi namjenske IKT sustave trebalo unaprijed razviti i uvesti. Ovom se Uredbom stoga predviđa hibridni model financiranja, pri čemu bi se nadzorni okvir kao takav u potpunosti financirao iz naknada, dok bi se razvoj IKT sustavâ europskih nadzornih tijela financirao iz doprinosâ Unije i nacionalnih nadležnih tijela.

(97) Nadležna tijela trebala bi imati sve potrebne ovlasti nadzora, istrage i sankcioniranja kako bi osigurala pravilno izvršavanje svojih zadaća na temelju ove Uredbe. U načelu bi trebala objavljivati obavijesti o administrativnim kaznama koje izreknu. Budući da financijski subjekti i treće strane pružatelji IKT usluga mogu imati poslovni nastan u različitim državama članicama i biti pod nadzorom različitih nadležnih tijela, primjenu ove Uredbe trebalo bi olakšati, s jedne strane, bliskom suradnjom među relevantnim nadležnim tijelima, uključujući ESB u pogledu posebnih zadaća koje su mu dodijeljene Uredbom Vijeća (EU) br. 1024/2013, i, s druge strane, savjetovanjem s europskim nadzornim tijelima putem uzajamne razmjene informacija i pružanja pomoći u kontekstu relevantnih nadzornih aktivnosti.

(98) Kako bi se dodatno kvantificirali i kvalificirali kriteriji za imenovanje trećih strana pružatelja IKT usluga kao ključnih te kako bi se uskladile naknade za nadzor, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a kako bi se ova Uredba dopunila dodatnim utvrđivanjem sistemskog učinka koji bi prekid ili operativni ispad treće strane pružatelja IKT usluga mogao imati na financijske subjekte kojima ta treća strana pruža IKT usluge, broja globalnih sistemski važnih institucija (GSV institucija) ili ostalih sistemski važnih institucija (OSV institucija) koje se oslanjaju na dotičnu treću stranu pružatelja IKT usluga, broja trećih strana pružatelja IKT usluga aktivnih na određenom tržištu, troškova migracije podataka i radnog opterećenja u području IKT-a na druge treće strane pružatelje IKT usluga, kao i iznosa naknada za nadzor i načina njihova plaćanja. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016. ([22]). Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće trebali bi primiti sve dokumente istodobno kada i stručnjaci iz država članica te bi njihovi stručnjaci sustavno trebali imati pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

(99) Regulatornim tehničkim standardima trebalo bi se osigurati dosljedno usklađivanje zahtjeva utvrđenih u ovoj Uredbi. Kao tijela s visokospecijaliziranim stručnim znanjem europska nadzorna tijela trebala bi izraditi nacrt regulatornih tehničkih standarda koji ne uključuje odabire u pogledu politika i dostaviti ga Komisiji. Trebalo bi razviti regulatorne tehničke standarde u područjima upravljanja IKT rizicima, izvješćivanja i testiranja u vezi sa značajnim IKT incidentima te u pogledu ključnih zahtjeva za dobro praćenje IKT rizika povezanog s trećim stranama. Komisija i europska nadzorna tijela trebali bi osigurati da te standarde i zahtjeve mogu primjenjivati svi financijski subjekti na način koji je razmjeran njihovoj veličini i ukupnom profilu rizičnosti te prirodi, opsegu i složenosti njihovih usluga, aktivnosti i poslovanja. Komisija bi trebala biti ovlaštena za donošenje tih regulatornih tehničkih standarda putem delegiranih akata na temelju članka 290. UFEU-a i u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

(100) Kako bi se poboljšala usporedivost izvješćâ o značajnim IKT incidentima i značajnim operativnim incidentima ili sigurnosnim incidentima povezanima s plaćanjem te osigurala transparentnost u pogledu ugovornih aranžmana za upotrebu IKT usluga koje pružaju treće strane pružatelji IKT usluga, europska nadzorna tijela trebala bi izraditi nacrt provedbenih tehničkih standarda kojima se utvrđuju standardizirani predlošci, obrasci i postupci za financijske subjekte za izvješćivanje o značajnom IKT incidentu i značajnom operativnom ili sigurnosnom incidentu povezanom s plaćanjem, kao i standardizirani predlošci za registar informacija. Pri izradi tih standarda europska nadzorna tijela trebala bi uzeti u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja. Komisija bi trebala biti ovlaštena za donošenje tih provedbenih tehničkih standarda putem provedbenih akata na temelju članka 291. UFEU-a i u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

([22]) SL L 123, 12.5.2016., str. 1.

(101) Budući da su dodatni zahtjevi već utvrđeni delegiranim i provedbenim aktima na temelju regulatornih i provedbenih tehničkih standarda u uredbama (EZ) br. 1060/2009 ([23]), (EU) br. 648/2012 ([24]), (EU) br. 600/2014 ([25]) i (EU) br. 909/2014 ([26]) Europskog parlamenta i Vijeća, primjereno je ovlastiti europska nadzorna tijela da zasebno ili zajednički u okviru Zajedničkog odbora podnose Komisiji regulatorne i provedbene tehničke standarde radi donošenja delegiranih i provedbenih akata kojima se prenose i ažuriraju postojeća pravila za upravljanje IKT rizicima.

(102) Budući da ova Uredba, zajedno s Direktivom (EU) 2022/2556 Europskog parlamenta i Vijeća ([27]), uključuje konsolidaciju odredaba o upravljanju IKT rizicima iz više uredbi i direktiva iz pravne stečevine Unije u području financijskih usluga, uključujući uredbe (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 (EU) i (EU) br. 909/2014 te Uredbu (EU) 2016/1011 Europskog parlamenta i Vijeća ([28]), kako bi se osigurala potpuna dosljednost navedene bi uredbe trebalo izmijeniti kako bi se pojasnilo da su primjenjive odredbe o IKT rizicima utvrđene u ovoj Uredbi.

(103) Stoga bi trebalo suziti područje primjene relevantnih članaka povezanih s operativnim rizikom na temelju kojih se ovlaštenjima utvrđenima u uredbama (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 predvidjelo donošenje delegiranih i provedbenih akata, kako bi se u ovu Uredbu prenijele sve odredbe koje obuhvaćaju aspekte digitalne operativne otpornosti koji su trenutačno dio tih uredbi.

(104) Potencijalni sistemski kiberrizik povezan s upotrebom IKT infrastruktura koje omogućuju rad platnih sustava i osiguravanje aktivnosti obrade plaćanja trebalo bi na odgovarajući način rješavati na razini Unije usklađenim pravilima o digitalnoj otpornosti. U tu bi svrhu Komisija trebala brzo procijeniti potrebu za preispitivanjem područja primjene ove Uredbe i istodobno uskladiti takvo preispitivanje s ishodom sveobuhvatnog preispitivanja predviđenog Direktivom (EU) 2015/2366. Brojni opsežni napadi tijekom posljednjeg desetljeća pokazuju kako su platni sustavi postali izloženi kiberprijetnjama. Budući da su u središtu lanca platnih usluga i snažno povezani s cjelokupnim financijskim sustavom, platni sustavi i aktivnosti obrade plaćanja postali su izuzetno važni za funkcioniranje financijskih tržišta Unije. Kibernapadi na takve sustave mogu uzrokovati ozbiljne poremećaje u poslovanju i imati izravne posljedice na ključne gospodarske funkcije, kao što je olakšavanje plaćanja, i neizravne učinke na povezane gospodarske procese. Dok se na razini Unije ne uspostave usklađeni režim i nadzor nad operatorima platnih sustava i izvršiteljima obrade, države članice mogu se, u cilju primjene sličnih tržišnih praksi, poslužiti zahtjevima u pogledu digitalne operativne otpornosti utvrđenima ovom Uredbom kad primjenjuju pravila na operatore platnih sustava i izvršitelje obrade koji su predmet nadzora u svojim jurisdikcijama.

([23]) Uredba (EZ) br. 1060/2009 Europskog parlamenta i Vijeća od 16. rujna 2009. o agencijama za kreditni rejting (SL L 302, 17.11.2009., str. 1.).

([24]) 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.).

([25]) Uredba (EU) br. 600/2014 Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Uredbe (EU) br. 648/2012 (SL L 173, 12.6.2014., str. 84.).

([26]) 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.).

([27]) Direktiva (EU) 2022/2556 Europskog parlamenta i Vijeća od 14. prosinca 2022. o izmjeni direktiva 2009/65/EZ, 2009/138/EZ, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 i (EU) 2016/2341 u pogledu digitalne operativne otpornosti za financijski sektor (vidjeti stranicu 153.. ovoga Službenog lista).

([28]) Uredba (EU) 2016/1011 Europskog parlamenta i Vijeća od 8. lipnja 2016. o indeksima koji se upotrebljavaju kao referentne vrijednosti u financijskim instrumentima i financijskim ugovorima ili za mjerenje uspješnosti investicijskih fondova i o izmjeni direktiva 2008/48/EZ i 2014/17/EU te Uredbe (EU) br. 596/2014 (SL L 171, 29.6.2016., str. 1.).

(105) S obzirom na to da cilj ove Uredbe, to jest postizanje visoke razine digitalne operativne otpornosti reguliranih financijskih subjekata, ne mogu dostatno ostvariti države članice jer on zahtijeva usklađivanje različitih pravila u pravu Unije i nacionalnom pravu, nego se zbog njegova opsega i učinaka on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

(106) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([29]) te je on dao mišljenje 10. svibnja 2021. ([30]),

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

Opće odredbe

Članak 1.

Predmet

1. Kako bi se postigla visoka zajednička razina digitalne operativne otpornosti, ovom se Uredbom utvrđuju jedinstveni zahtjevi u pogledu sigurnosti mrežnih i informacijskih sustava kojima se podupiru poslovni procesi financijskih subjekata kako slijedi:

(a) zahtjevi primjenjivi na financijske subjekte koji se odnose na:

   i. upravljanje rizikom informacijske i komunikacije tehnologije (IKT);

   ii. izvješćivanje o značajnim IKT incidentima i dobrovoljno obavješćivanje nadležnih tijela o ozbiljnim kiberprijetnjama;

   iii. izvješćivanje nadležnih tijela, od strane financijskih subjekata iz članka 2. stavka 1. točaka od (a) do (d), o značajnim operativnim ili sigurnosnim incidentima povezanima s plaćanjem;

   iv. testiranje digitalne operativne otpornosti;

   v. razmjenu informacija i saznanja o kiberprijetnjama i ranjivostima;

   vi. mjere za dobro upravljanje IKT rizikom povezanim s trećim stranama;

(b) zahtjevi koji se odnose na ugovorne aranžmane sklopljene između trećih strana pružatelja IKT usluga i financijskih subjekata;

(c) pravila za uspostavu i provedbu nadzornog okvira za ključne treće strane pružatelje IKT usluga pri pružanju usluga financijskim subjektima;

(d) pravila za suradnju među nadležnim tijelima i pravila o nadzoru i izvršavanju koje provode nadležna tijela u vezi sa svim pitanjima obuhvaćenima ovom Uredbom.

2. Kad je riječ o financijskim subjektima koji su identificirani kao ključnih ili važni subjekti na temelju nacionalnih propisa kojima se prenosi članak 3. Direktive (EU) 2022/2555, ova Uredba smatra se sektorskim pravnim aktom Unije za potrebe članka 4. te direktive.

3. Ovom se Uredbom ne dovodi u pitanje odgovornost država članica u vezi s temeljnim državnim funkcijama koje se odnose na javnu sigurnost, obranu i nacionalnu sigurnost u skladu s pravom Unije.

([29]) Uredba (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.).

([30]) SL C 229, 15.6.2021., str. 16.

Članak 2.

Područje primjene

1. Ne dovodeći u pitanje stavke 3. i 4., ova se Uredba primjenjuje na sljedeće subjekte:

(a) kreditne institucije;

(b) institucije za platni promet, uključujući institucije za platni promet izuzete na temelju Direktive (EU) 2015/2366;

(c) pružatelje usluga pružanja informacija o računu;

(d) institucije za elektronički novac, uključujući institucije za elektronički novac izuzete na temelju Direktive 2009/110/EZ;

(e) investicijska društva;

(f) pružatelje usluga povezanih s kriptoimovinom koji imaju odobrenje za rad na temelju uredbe Europskog parlamenta i Vijeća o tržištima kriptoimovine i izmjeni uredaba (EU) br. 1093/2010 i (EU) br. 1095/2010 te direktiva 2013/36/EU i (EU) 2019/1937 („Uredba o tržištima kriptoimovine”) i izdavatelje tokena vezanih uz imovinu;

(g) središnje depozitorije vrijednosnih papira;

(h) središnje druge ugovorne strane;

(i) mjesta trgovanja;

(j) trgovinske repozitorije;

(k) upravitelje alternativnih investicijskih fondova;

(l) društva za upravljanje;

(m) pružatelje usluga dostave podataka;

(n) društva za osiguranje i društva za reosiguranje;

(o) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju;

(p) institucije za strukovno mirovinsko osiguranje;

(q) agencije za kreditni rejting;

(r) administratore ključnih referentnih vrijednosti;

(s) pružatelje usluga skupnog financiranja;

(t) sekuritizacijske repozitorije;

(u) treće strane pružatelje IKT usluga.

2. Za potrebe ove Uredbe subjekti iz stavka 1. točaka od (a) do (t) zajednički se nazivaju „financijski subjekti”.

3. Ova se Uredba ne primjenjuje na:

(a) upravitelje alternativnih investicijskih fondova iz članka 3. stavka 2. Direktive 2011/61/EU;

(b) društva za osiguranje i društva za reosiguranje iz članka 4. Direktive 2009/138/EZ;

(c) institucije za strukovno mirovinsko osiguranje koje upravljaju mirovinskim programima koji zajedno nemaju više od ukupno 15 članova;

(d) fizičke ili pravne osobe izuzete na temelju članaka 2. i 3. Direktive 2014/65/EU;

(e) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju koji su mikropoduzeća ili mala ili srednja poduzeća;

(f) poštanske žiro institucije iz članka 2. stavka 5. točke 3. Direktive 2013/36/EU.

4. Države članice mogu iz područja primjene ove Uredbe isključiti subjekte iz članka 2. stavka 5. točaka od 4. do 23. Direktive 2013/36/EU koji se nalaze na njihovu državnom području. Ako država članica iskoristi tu mogućnost, ona o tome i o svim kasnijim promjenama obavješćuje Komisiju. Komisija te informacije objavljuje na svojim internetskim stranicama ili na drugi lako dostupan način.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „digitalna operativna otpornost” znači sposobnost financijskog subjekta da izgradi, osigura i preispituje svoju operativnu cjelovitost i pouzdanost tako da upotrebom usluga koje pružaju treće strane pružatelji IKT usluga izravno ili neizravno osigura cijeli raspon IKT sposobnosti potrebnih za sigurnost mrežnih i informacijskih sustava kojima se financijski subjekt koristi i kojima se podupire kontinuirano pružanje financijskih usluga i njihova kvaliteta, među ostalim i tijekom poremećaja;

2. „mrežni i informacijski sustav” znači mrežni i informacijski sustav kako je definiran u članku 6. točki 1. Direktive (EU) 2022/2555;

3. „zastarjeli IKT sustav” znači IKT sustav koji je na kraju svojeg životnog ciklusa, a koji zbog tehnoloških ili komercijalnih razloga nije prikladan za nadogradnju ili popravak ili za koji njegov dobavljač ili treća strana pružatelj IKT usluga više ne pruža podršku, ali je još uvijek u upotrebi i podržava funkcije financijskog subjekta;

4. „sigurnost mrežnih i informacijskih sustava” znači sigurnost mrežnih i informacijskih sustava kako je definirana u članku 6. točki 2. Direktive (EU) 2022/2555;

5. „IKT rizik” znači svaka razumno prepoznatljiva okolnost koja se odnosi na upotrebu mrežnih i informacijskih sustava, koja, ako do nje dođe, može dovesti do negativnih učinaka u digitalnom ili fizičkom okruženju te time ugroziti sigurnost mrežnih i informacijskih sustava, svih alata ili procesa koji ovise o tehnologiji, operacija i procesa ili pružanja usluga;

6. „informacijska imovina” znači skup materijalnih ili nematerijalnih informacija koje vrijedi zaštititi;

7. „IKT imovina” znači softverska ili hardverska imovina u mrežnim i informacijskim sustavima koju upotrebljava financijski subjekt;

8. „IKT incident” znači događaj ili niz povezanih događaja koje financijski subjekt nije planirao i koji ugrožavaju sigurnost mrežnih i informacijskih sustava i negativno utječu na dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka, ili na usluge koje pruža financijski subjekt;

9. „operativni ili sigurnosni incident povezan s plaćanjem” znači događaj ili niz povezanih događaja, neovisno o tome jesu li povezani s IKT-om ili ne, koje financijski subjekti iz članka 2. stavka 1. točaka od (a) do (d) nisu planirali i koji negativno utječu na dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka povezanih s plaćanjem ili na usluge povezane s plaćanjem koje pruža financijski subjekt;

10. „značajan IKT incident” znači IKT incident koji izrazito negativno utječe na mrežne i informacijske sustave kojima se podupiru ključne ili važne funkcije financijskog subjekta;

11. „značajan operativni ili sigurnosni incident povezan s plaćanjem” znači operativni ili sigurnosni incident koji izrazito negativno utječe na pružene usluge povezane s plaćanjem;

12. „kiberprijetnja” znači kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;

13. „ozbiljna kiberprijetnja” znači kiberprijetnja čije tehničke značajke ukazuju na to da je mogla dovesti do značajnog IKT incidenta ili značajnog operativnog ili sigurnosnog incidenta povezanog s plaćanjem;

14. „kibernapad” znači zlonamjeran IKT incident uzrokovan pokušajem bilo kojeg aktera prijetnje da uništi, izloži, izmijeni, onemogući, ukrade ili neovlašteno koristi imovinu ili joj neovlašteno pristupi;

15. „saznanja o prijetnjama” znači informacije koje su agregirane, preoblikovane, analizirane, protumačene ili obogaćene kako bi se dobio kontekst potreban za donošenje odluka i kako bi se omogućilo relevantno i dostatno razumijevanje za ublažavanje učinka IKT incidenta ili kiberprijetnje, uključujući tehničke pojedinosti kibernapada, onih koji su odgovorni za napad te njihova načina rada i njihovih motiva;

16. „ranjivost” znači slabost, osjetljivost ili nedostatak neke imovine, sustava, procesa ili kontrole koji se može iskoristiti;

17. „penetracijska testiranja vođena prijetnjama (TLPT)” znači okvir koji oponaša taktike, tehnike i procedure stvarnih aktera prijetnje koje se smatraju stvarnom kiberprijetnjom, koji omogućuje kontrolirano, prilagođeno testiranje ključnih produkcijskih sustava financijskog subjekta, vođeno saznanjima o prijetnjama („crveni tim”);

18. „IKT rizik povezan s trećim stranama” znači IKT rizik koji može nastati za financijski subjekt u vezi s upotrebom IKT usluga koje pružaju treće strane pružatelji IKT usluga ili njihovi podugovaratelji, među ostalim i putem aranžmana za eksternalizaciju;

19. „treća strana pružatelj IKT usluga” znači poduzetnik koji pruža IKT usluge;

20. „pružatelj IKT usluga unutar grupe” znači društvo koje je dio financijske grupe i koje uglavnom pruža IKT usluge financijskim subjektima unutar iste grupe ili financijskim subjektima koji pripadaju istom institucionalnom sustavu zaštite, među ostalim i njihovim matičnim društvima, društvima kćerima, podružnicama ili drugim subjektima koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom;

21. „IKT usluge” znači digitalne i podatkovne usluge koje se putem IKT sustavâ kontinuirano pružaju jednom ili više unutarnjih ili vanjskih korisnika, uključujući usluge najma informatičke opreme (engl. *hardware as a service*) i hardverske usluge koje uključuju pružanje tehničke podrške od strane pružatelja hardvera putem ažuriranja softvera ili ugrađenog softvera, uz iznimku tradicionalnih analognih telefonskih usluga;

22. „ključna ili važna funkcija” znači funkcija čiji bi poremećaj bitno narušio financijske rezultate financijskog subjekta ili pouzdanost ili kontinuitet njegovih usluga i aktivnosti, odnosno funkcija čiji bi prestanak, neispravnost ili neizvršenje bitno narušili sposobnost financijskog subjekta da kontinuirano ispunjava uvjete i obveze iz svojeg odobrenja za rad ili druge obveze na temelju primjenjivog prava o financijskim uslugama;

23. „ključna treća strana pružatelj IKT usluga” znači treća strana pružatelj IKT usluga imenovana kao ključna u skladu s člankom 31.;

24. „treća strana pružatelj IKT usluga s poslovnim nastanom u trećoj zemlji” znači treća strana pružatelj IKT usluga koja je pravna osoba s poslovnim nastanom u trećoj zemlji, a koja je s financijskim subjektom sklopila ugovorni aranžman o pružanju IKT usluga;

25. „društvo kći” znači poduzeće kći u smislu članka 2. točke 10. i članka 22. Direktive 2013/34/EU;

26. „grupa” znači grupa kako je definirana u članku 2. točki 11. Direktive 2013/34/EU;

27. „matično društvo” znači matično poduzeće u smislu članka 2. točke 9. i članka 22. Direktive 2013/34/EU;

28. „podugovaratelj IKT usluga s poslovnim nastanom u trećoj zemlji” znači podugovaratelj IKT-a koji je pravna osoba s poslovnim nastanom u trećoj zemlji, a koji je sklopio ugovorni aranžman s trećom stranom pružateljem IKT usluga ili s trećom stranom pružateljem IKT usluga s poslovnim nastanom u trećoj zemlji;

29. „koncentracijski IKT rizik” znači izloženost prema jednoj ili više povezanih ključnih trećih strana pružatelja IKT usluga, čime se stvara određeni stupanj ovisnosti o takvim pružateljima tako da nedostupnost, prekid ili neka druga vrsta nedostatka tih pružatelja može potencijalno ugroziti sposobnost financijskog subjekta za obavljanje ključnih ili važnih funkcija ili može dovesti do drugih vrsta negativnih učinaka, među ostalim i velikih gubitaka, ili može ugroziti financijsku stabilnost Unije u cjelini;

30. „upravljačko tijelo” znači upravljačko tijelo kako je definirano u članku 4. stavku 1. točki 36. Direktive 2014/65/EU, članku 3. stavku 1. točki 7. Direktive 2013/36/EU, članku 2. stavku 1. točki (s) Direktive 2009/65/EZ Europskog parlamenta i Vijeća ([31]), članku 2. stavku 1. točki 45. Uredbe (EU) br. 909/2014, članku 3. stavku 1. točki 20. Uredbe (EU) 2016/1011 te u relevantnoj odredbi Uredbe o tržištima kriptoimovine ili ekvivalentne osobe koje u praksi upravljaju subjektom ili imaju ključne funkcije u skladu s relevantnim pravom Unije ili nacionalnim pravom;

31. „kreditna institucija” znači kreditna institucija kako je definirana u članku 4. stavku 1. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća ([32]);

32. „institucija izuzeta na temelju Direktive 2013/36/EU” znači subjekt iz članka 2. stavka 5. točaka od 4. do 23. Direktive 2013/36/EU;

33. „investicijsko društvo” znači investicijsko društvo kako je definirano u članku 4. stavku 1. točki 1. Direktive 2014/65/EU;

34. „malo i nepovezano investicijsko društvo” znači investicijsko društvo koje ispunjava uvjete utvrđene u članku 12. stavku 1. Uredbe (EU) 2019/2033 Europskog parlamenta i Vijeća ([33]);

35. „institucija za platni promet” znači institucija za platni promet kako je definirana u članku 4. točki 4. Direktive (EU) 2015/2366;

36. „institucija za platni promet izuzeta na temelju Direktive 2015/2366” znači institucija za platni promet izuzeta na temelju članka 32. stavka 1. Direktive (EU) 2015/2366;

37. „pružatelj usluga pružanja informacija o računu” znači pružatelj usluga pružanja informacija o računu iz članka 33. stavka 1. Direktive (EU) 2015/2366;

38. „institucija za elektronički novac” znači institucija za elektronički novac kako je definirana u članku 2. točki 1. Direktive 2009/110/EZ;

39. „institucija za elektronički novac izuzeta na temelju Direktive 2009/110/EZ” znači institucija za elektronički novac na koju se primjenjuje izuzeće iz članka 9. stavka 1. Direktive 2009/110/EZ;

40. „središnja druga ugovorna strana” znači središnja druga ugovorna strana kako je definirana u članku 2. točki 1. Uredbe (EU) br. 648/2012;

41. „trgovinski repozitorij” znači trgovinski repozitorij kako je definiran u članku 2. točki 2. Uredbe (EU) br. 648/2012;

42. „središnji depozitorij vrijednosnih papira” znači središnji depozitorij vrijednosnih papira kako je definiran u članku 2. stavku 1. točki 1. Uredbe (EU) br. 909/2014;

43. „mjesto trgovanja” znači mjesto trgovanja kako je definirano u članku 4. stavku 1. točki 24. Direktive 2014/65/EU;

44. „upravitelj alternativnih investicijskih fondova” znači upravitelj alternativnih investicijskih fondova kako je definiran u članku 4. stavku 1. točki (b) Direktive 2011/61/EU;

45. „društvo za upravljanje” znači društvo za upravljanje kako je definirano u članku 2. stavku 1. točki (b) Direktive 2009/65/EZ;

46. „pružatelj usluga dostave podataka” znači pružatelj usluga dostave podataka u smislu Uredbe (EU) br. 600/2014, kako je naveden u njezinu članku 2. stavku 1. točkama od 34. do 36.;

47. „društvo za osiguranje” znači društvo za osiguranje kako je definirano u članku 13. točki 1. Direktive 2009/138/EZ;

48. „društvo za reosiguranje” znači društvo za reosiguranje kako je definirano u članku 13. točki 4. Direktive 2009/138/EZ;

([31]) Direktiva 2009/65/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju zakona i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (UCITS) (SL L 302, 17.11.2009., str. 32.).

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

([33]) Uredba (EU) 2019/2033 Europskog parlamenta i Vijeća od 27. studenoga 2019. o bonitetnim zahtjevima za investicijska društva i o izmjeni uredaba (EU) br. 1093/2010, (EU) br. 575/2013, (EU) br. 600/2014 i (EU) br. 806/2014 (SL L 314, 5.12.2019., str. 1.).

49. „posrednik u osiguranju” znači posrednik u osiguranju kako je definiran u članku 2. stavku 1. točki 3. Direktive (EU) 2016/97 Europskog parlamenta i Vijeća ([34]);

50. „sporedni posrednik u osiguranju” znači sporedni posrednik u osiguranju kako je definiran u članku 2. stavku 1. točki 4. Direktive (EU) 2016/97;

51. „posrednik u reosiguranju” znači posrednik u reosiguranju kako je definiran u članku 2. stavku 1. točki 5. Direktive (EU) 2016/97;

52. „institucija za strukovno mirovinsko osiguranje” znači institucija za strukovno mirovinsko osiguranje kako je definirana u članku 6. točki 1. Direktive (EU) 2016/2341;

53. „mala institucija za strukovno mirovinsko osiguranje” znači institucija za strukovno mirovinsko osiguranje koja upravlja mirovinskim programima koji ukupno imaju manje od 100 članova;

54. „agencija za kreditni rejting” znači agencija za kreditni rejting kako je definirana u članku 3. stavku 1. točki (b) Uredbe (EZ) br. 1060/2009;

55. „pružatelj usluga povezanih s kriptoimovinom” znači pružatelj usluga povezanih s kriptoimovinom kako je definiran u relevantnoj odredbi Uredbe o tržištima kriptoimovine;

56. „izdavatelj tokena vezanih uz imovinu” znači izdavatelj tokena vezanih uz imovinu kako je definiran u relevantnoj odredbi Uredbe o tržištima kriptoimovine;

57. „administrator ključnih referentnih vrijednosti” znači administrator „ključnih referentnih vrijednosti” kako su definirane u članku 3. točki 25. Uredbe (EU) 2016/1011;

58. „pružatelj usluga skupnog financiranja” znači pružatelj usluga skupnog financiranja kako je definiran u članku 2. stavku 1. točki (e) Uredbe (EU) 2020/1503 Europskog parlamenta i Vijeća ([35]);

59. „sekuritizacijski repozitorij” znači sekuritizacijski repozitorij kako je definiran u članku 2. točki 23. Uredbe (EU) 2017/2402 Europskog parlamenta i Vijeća ([36]);

60. „mikropoduzeće” znači financijski subjekt koji nije mjesto trgovanja, središnja druga ugovorna strana, trgovinski repozitorij ili središnji depozitorij vrijednosnih papira, a koji zapošljava manje od 10 osoba i čiji ukupni godišnji promet i/ili ukupna godišnja bilanca ne premašuje 2 milijuna EUR;

61. „glavno nadzorno tijelo” znači europsko nadzorno tijelo imenovano u skladu s člankom 31. stavkom 1. točkom (b) ove Uredbe;

62. „Zajednički odbor” znači odbor iz članka 54. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010;

63. „malo poduzeće” znači financijski subjekt koji zapošljava 10 ili više osoba, ali manje od 50 osoba i čiji ukupni godišnji promet i/ili čija ukupna godišnja bilanca premašuje 2 milijuna EUR, ali ne premašuje 10 milijuna EUR;

64. „srednje poduzeće” znači financijski subjekt koji nije malo poduzeće, koji zapošljava manje od 250 osoba i čiji godišnji promet ne premašuje 50 milijuna EUR i/ili čija godišnja bilanca ne premašuje 43 milijuna EUR;

65. „tijelo javne vlasti” znači svako državno tijelo ili drugo tijelo javne uprave, uključujući nacionalne središnje banke.

([34]) Direktiva (EU) 2016/97 Europskog parlamenta i Vijeća od 20. siječnja 2016. o distribuciji osiguranja (SL L 26, 2.2.2016., str. 19.).

([35]) Uredba (EU) 2020/1503 Europskog parlamenta i Vijeća od 7. listopada 2020. o europskim pružateljima usluga skupnog financiranja za poduzeća i izmjeni Uredbe (EU) 2017/1129 i Direktive (EU) 2019/1937 (SL L 347, 20.10.2020., str. 1.).

([36]) Uredba (EU) 2017/2402 Europskog parlamenta i Vijeća od 12. prosinca 2017. o utvrđivanju općeg okvira za sekuritizaciju i o uspostavi specifičnog okvira za jednostavnu, transparentnu i standardiziranu sekuritizaciju te o izmjeni direktiva 2009/65/EZ, 2009/138/EZ i 2011/61/EU te uredaba (EZ) br. 1060/2009 i (EU) br. 648/2012 (SL L 347, 28.12.2017., str. 35.).

Članak 4.

Načelo proporcionalnosti

1. Financijski subjekti provode pravila utvrđena u poglavlju II. u skladu s načelom proporcionalnosti, uzimajući u obzir svoju veličinu i ukupni profil rizičnosti te prirodu, opseg i složenost svojih usluga, aktivnosti i poslovanja.

2. Osim toga, financijski subjekti primjenjuju poglavlja III. i IV. te poglavlje V. odjeljak I. razmjerno svojoj veličini i ukupnom profilu rizičnosti te prirodi, opsegu i složenosti svojih usluga, aktivnosti i poslovanja, kako je konkretno predviđeno u relevantnim pravilima iz tih poglavlja.

3. Pri preispitivanju dosljednosti okvira za upravljanje IKT rizicima na temelju izvješća podnesenih na zahtjev nadležnih tijela u skladu s člankom 6. stavkom 5. i člankom 16. stavkom 2., nadležna tijela razmatraju jesu li financijski subjekti primijenili načelo proporcionalnosti.

POGLAVLJE II.

Upravljanje IKT rizicima

Odjeljak I.

Članak 5.

Upravljanje i organizacija

1. Financijski subjekti uspostavljaju okvir za unutarnje upravljanje i kontrolu kojim se osigurava djelotvorno i razborito upravljanje IKT rizicima, u skladu s člankom 6. stavkom 4., kako bi se postigla visoka razina digitalne operativne otpornosti.

2. Upravljačko tijelo financijskog subjekta utvrđuje, odobrava i nadzire sve aranžmane povezane s okvirom za upravljanje IKT rizicima iz članka 6. stavka 1. te je odgovorno za njihovu provedbu.

Za potrebe prvog podstavka upravljačko tijelo:

(a) snosi krajnju odgovornost za upravljanje IKT rizicima financijskog subjekta;

(b) uspostavlja politike čiji je cilj osigurati održavanje visokih standarda dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka;

(c) određuje jasne uloge i odgovornosti za sve funkcije povezane s IKT-om i uspostavlja odgovarajuće aranžmane upravljanja kako bi se osigurale djelotvorna i pravodobna komunikacija, suradnja i koordinacija među tim funkcijama;

(d) snosi opću odgovornost za utvrđivanje i odobravanje strategije za digitalnu operativnu otpornost iz članka 6. stavka 8., među ostalim i za određivanje odgovarajuće razine tolerancije financijskog subjekta na IKT rizik, kako je navedeno u članku 6. stavku 8. točki (b);

(e) odobrava, nadzire i periodički preispituje način na koji financijski subjekt provodi politiku kontinuiteta poslovanja u području IKT-a te planove odgovora i oporavka u području IKT-a iz članka 11. stavka 1. odnosno stavka 3., pri čemu se ta politika može donijeti kao zasebna politika koja je sastavni dio cjelokupne politike kontinuiteta poslovanja te plana odgovora i oporavka financijskog subjekta;

(f) odobrava i periodički preispituje planove financijskog subjekta za unutarnju reviziju u području IKT-a, revizije u području IKT-a i njihove bitne izmjene;

(g) izrađuje i periodički preispituje odgovarajući proračun za ispunjavanje potreba financijskog subjekta u pogledu digitalne operativne otpornosti, i to za sve vrste resursa, što uključuje relevantne programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti iz članka 13. stavka 6. te stjecanje vještina u području IKT-a za sve članove osoblja;

(h) odobrava i periodički preispituje politiku financijskog subjekta u vezi s aranžmanima za upotrebu IKT usluga koje pružaju treće strane pružatelji IKT usluga;

(i) na korporativnoj razini uspostavlja kanale za izvješćivanje s pomoću kojih će moći biti propisno obaviješteno o sljedećem:

i. aranžmanima o upotrebi IKT usluga sklopljenima s trećim stranama pružateljima IKT usluga;

ii. svim relevantnim planiranim bitnim promjenama u pogledu trećih strana pružatelja IKT usluga;

iii. potencijalnom učinku takvih promjena na ključne ili važne funkcije obuhvaćene tim aranžmanima, što uključuje sažetak analize rizika kako bi se procijenio učinak tih promjena; i barem o značajnim IKT incidentima i njihovu učinku kao i o odgovoru, oporavku i korektivnim mjerama.

3. Financijski subjekti koji nisu mikropoduzeća uvode funkciju za praćenje aranžmana o upotrebi IKT usluga sklopljenih s trećim stranama pružateljima IKT usluga ili imenuju člana višeg rukovodstva koji će biti odgovoran za nadzor nad povezanom izloženosti rizicima i relevantnom dokumentacijom.

4. Članovi upravljačkog tijela financijskog subjekta aktivno osvježavaju znanje i vještine koji su im dostatni kako bi mogli razumjeti i procijeniti IKT rizik i njegov učinak na poslovanje financijskog subjekta, među ostalim i tako da redovito pohađaju posebno osposobljavanje, razmjerno IKT riziku kojima se upravlja.

Odjeljak II.

Članak 6.

Okvir za upravljanje IKT rizicima

1. Financijski subjekti u sklopu svojeg općeg sustava za upravljanje rizicima imaju pouzdan, sveobuhvatan i dobro dokumentiran okvir za upravljanje IKT rizicima, koji im omogućuje brzo, učinkovito i sveobuhvatno odgovaranje na IKT rizik te osigurava visoku razinu digitalne operativne otpornosti.

2. Okvir za upravljanje IKT rizicima obuhvaća barem strategije, politike, postupke te IKT protokole i alate koji su potrebni za propisnu i primjerenu zaštitu sve informacijske imovine i IKT imovine, što uključuje računalni softver, hardver i poslužitelje, te za zaštitu svih relevantnih fizičkih komponenata i infrastrukture, kao što su prostori, podatkovni centri i područja određena kao osjetljiva, kako bi se osiguralo da je sva informacijska imovina i IKT imovina primjereno zaštićena od rizikâ, među ostalim i od oštećenja te neovlaštenog pristupa ili upotrebe.

3. Financijski subjekti, u skladu sa svojim okvirom za upravljanje IKT rizicima, svode učinak IKT rizika na najmanju moguću mjeru uvođenjem odgovarajućih strategija, politika, postupaka, IKT protokola i alata. Financijski subjekti dostavljaju nadležnim tijelima potpune i ažurirane informacije o IKT rizicima i o svojem okviru za upravljanje IKT rizicima na zahtjev tih tijela.

4. Financijski subjekti koji nisu mikropoduzeća odgovornost za upravljanje IKT rizicima i nadzor nad njima dodjeljuju kontrolnoj funkciji i osiguravaju odgovarajuću razinu neovisnosti takve kontrolne funkcije kako bi se izbjegli sukobi interesa. Financijski subjekti osiguravaju odgovarajuće razdvajanje i neovisnost funkcija upravljanja IKT rizicima, kontrolnih funkcija i funkcija unutarnje revizije, u skladu s modelom „triju crta obrane” ili internim modelom upravljanja rizicima i kontrole nad njima.

5. Okvir za upravljanje IKT rizicima dokumentira se i preispituje najmanje jedanput godišnje, ili periodički ako je riječ o mikropoduzećima, kao i po nastanku značajnih IKT incidenata te u skladu s uputama ili zaključcima nadzornog tijela koji su izrađeni slijedom relevantnog testiranja digitalne operativne otpornosti ili revizijskih procesa. Kontinuirano ga se poboljšava na temelju pouka iz provedbe i praćenja. Izvješće o preispitivanju okvira za upravljanje IKT rizicima podnosi se nadležnom tijelu na njegov zahtjev.

6. Okvir za upravljanje IKT rizicima financijskih subjekata koji nisu mikropoduzeća podliježe redovitoj unutarnjoj reviziji, koju revizori provode u skladu s planom revizije financijskog subjekta. Ti revizori moraju imati dostatno znanje, vještine i stručno znanje u području IKT rizika, kao i odgovarajuću neovisnost. Učestalost i težište revizija u području IKT-a moraju biti razmjerni IKT riziku financijskog subjekta.

7. Financijski subjekti na temelju zaključaka unutarnjeg revizijskog pregleda uspostavljaju formalni proces daljnjeg postupanja, uključujući pravila za pravodobnu provjeru i ispravljanje ključnih nalaza revizije u području IKT-a.

8. Okvir za upravljanje IKT rizicima obuhvaća strategiju za digitalnu operativnu otpornost, u kojoj je utvrđen način provedbe okvira. U tu svrhu strategija za digitalnu operativnu otpornost uključuje metode za odgovaranje na IKT rizik i ostvarenje posebnih ciljeva u području IKT-a na sljedeći način:

(a) objašnjava se kako se okvirom za upravljanje IKT rizicima podupiru poslovna strategija i ciljevi financijskog subjekta;

(b) utvrđuje se razina tolerancije na IKT rizik, u skladu sa sklonošću financijskog subjekta preuzimanju rizika, te se analizira učinak tolerancije za poremećaje u radu IKT-a;

(c) utvrđuju se jasni ciljevi u području informacijske sigurnosti, uključujući ključne pokazatelje uspješnosti i ključne parametre rizika;

(d) objašnjava se referentna IKT arhitektura i sve promjene koje su potrebne za ostvarenje specifičnih poslovnih ciljeva;

(e) u glavnim crtama izlažu se različiti mehanizmi uspostavljeni radi otkrivanja IKT incidenata, sprečavanja njihovih učinaka i pružanja zaštite od tih učinaka;

(f) jasno se prikazuje aktualna situacija u pogledu digitalne operativne otpornosti, i to na temelju broja prijavljenih značajnih IKT incidenata i djelotvornosti preventivnih mjera;

(g) uvodi se testiranje digitalne operativne otpornosti, u skladu s poglavljem IV. ove Uredbe;

(h) u glavnim crtama izlaže se komunikacijska strategija za slučaj IKT incidenata koji se moraju objaviti u skladu s člankom 14.

9. U kontekstu strategije za digitalnu operativnu otpornost iz stavka 8. financijski subjekti mogu utvrditi sveobuhvatnu strategiju za nabavu IKT-a od više dobavljača, na razini grupe ili subjekta, u kojoj se izlažu ključne ovisnosti o trećim stranama pružateljima IKT usluga i objašnjava razlog za mješovitu nabavu od različitih trećih strana pružatelja IKT usluga.

10. Financijski subjekti mogu, u skladu sa sektorskim pravom Unije i nacionalnim sektorskim pravom, eksternalizirati zadaće provjeravanja usklađenosti sa zahtjevima u pogledu upravljanja IKT rizicima društvima unutar grupe ili vanjskim društvima. U slučaju takve eksternalizacije financijski subjekt ostaje u potpunosti odgovoran za provjeru usklađenosti sa zahtjevima u pogledu upravljanja IKT rizicima.

Članak 7.

IKT sustavi, protokoli i alati

Kako bi odgovorili na IKT rizik i upravljali njime, financijski subjekti upotrebljavaju i održavaju ažuriranima IKT sustave, protokole i alate koji su:

(a) primjereni razmjeru operacija koje podupiru poslovanje tih financijskih subjekata, u skladu s načelom proporcionalnosti iz članka 4.;

(b) pouzdani;

(c) opremljeni dostatnim kapacitetom za pravilnu obradu podataka potrebnih za obavljanje aktivnosti i pravodobno pružanje usluga, kao i kapacitetom za najjače opterećenje nalozima, porukama ili transakcijama, ovisno o potrebi, među ostalim i u slučaju uvođenja nove tehnologije;

(d) tehnološki otporni da mogu primjereno ispuniti dodatne potrebe za obradom informacija u stresnim okolnostima na tržištu ili drugim nepovoljnim situacijama.

Članak 8.

Utvrđivanje

1. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. financijski subjekti utvrđuju, klasificiraju i na odgovarajući način dokumentiraju sve poslovne funkcije, uloge i odgovornosti koje se podupiru IKT-om, informacijsku imovinu i IKT imovinu kojom se te funkcije podupiru te njihove uloge i ovisnosti u odnosu na IKT rizik. Financijski subjekti prema potrebi, a najmanje jedanput godišnje, preispituju primjerenost te klasifikacije i sve relevantne dokumentacije.

2. Financijski subjekti kontinuirano utvrđuju sve izvore IKT rizika, osobito izloženost riziku drugih financijskih subjekata i od drugih financijskih subjekata, te procjenjuju kiberprijetnje i ranjivosti IKT-a koje su relevantne za njihove poslovne funkcije koje se podupiru IKT-om te za informacijsku imovinu i IKT imovinu. Financijski subjekti redovito, a najmanje jedanput godišnje, preispituju scenarije rizika koji utječu na njih.

3. Financijski subjekti koji nisu mikropoduzeća provode procjenu rizika nakon svake značajne promjene u infrastrukturi mrežnog i informacijskog sustava, u procesima ili postupcima koji utječu na njihove poslovne funkcije koje se podupiru IKT-om te informacijsku imovinu ili IKT imovinu.

4. Financijski subjekti utvrđuju svu informacijsku imovinu i IKT imovinu, među ostalima i onu na udaljenim lokacijama, mrežne resurse i hardversku opremu te mapiraju onu koju smatraju ključnom. Financijski subjekti mapiraju konfiguraciju informacijske imovine i IKT imovine te veze među različitom informacijskom imovinom i IKT imovinom i njihove međuovisnosti.

5. Financijski subjekti utvrđuju i dokumentiraju sve procese koji ovise o trećim stranama pružateljima IKT usluga te utvrđuju međusobnu povezanost s trećim stranama pružateljima IKT usluga koji pružaju usluge kojima se podupiru ključne ili važne funkcije.

6. Za potrebe stavaka 1., 4. i 5. financijski subjekti vode relevantne evidencije, koje ažuriraju redovito i svaki put kad dođe do značajnih promjena iz stavka 3.

7. Financijski subjekti koji nisu mikropoduzeća redovito, a najmanje jedanput godišnje, provode posebnu procjenu IKT rizika za sve zastarjele IKT sustave, a u svakom slučaju prije i nakon povezivanja tehnologija, aplikacija ili sustava.

Članak 9.

Zaštita i sprečavanje

1. Za potrebe primjerene zaštite IKT sustavâ i u cilju organiziranja mjera odgovora, financijski subjekti kontinuirano prate i kontroliraju sigurnost i funkcioniranje IKT sustavâ i alatâ te učinak IKT rizika na IKT sustave svode na najmanju moguću mjeru uvođenjem odgovarajućih alata, politika i postupaka za sigurnost IKT-a.

2. Financijski subjekti osmišljavaju, izrađuju i provode politike, postupke, protokole i alate za sigurnost IKT-a čiji je cilj osigurati otpornost, kontinuitet i dostupnost IKT sustava, posebno onih kojima se podupiru ključne ili važne funkcije, te održavati visoke standarde dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka, neovisno o tome jesu li u mirovanju, upotrebi ili prijenosu.

3. Kako bi ostvarili ciljeve iz stavka 2., financijski subjekti primjenjuju IKT rješenja i procese koji su primjereni u skladu s člankom 4. Tim IKT rješenjima i procesima:

(a) osigurava se sigurnost sredstava za prijenos podataka;

(b) na najmanju moguću mjeru svodi se rizik od oštećenja ili gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje;

(c) sprečavaju se pomanjkanje dostupnosti, narušavanje vjerodostojnosti i cjelovitosti, kršenja povjerljivosti i gubitak podataka;

(d) osigurava se zaštita podataka od rizika koji proizlaze iz upravljanja podatcima, među ostalim i iz loše administracije, rizika povezanih s obradom i ljudske pogreške.

4. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. financijski subjekti:

(a) razvijaju i dokumentiraju politiku informacijske sigurnosti kojom se utvrđuju pravila za zaštitu dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka te informacijske imovine i IKT imovine, među ostalim, ako je to primjenjivo, i podataka i te imovine njihovih klijenata;

(b) primjenom pristupa koji se temelji na procjeni rizika uspostavljaju pouzdanu strukturu za upravljanje mrežom i infrastrukturom s pomoću odgovarajućih tehnika, metoda i protokola, koji mogu uključivati automatizirane mehanizme za izoliranje zahvaćene informacijske imovine u slučaju kibernapadâ;

(c) provode politike kojima se fizički ili logički pristup informacijskoj i IKT imovini ograničava samo na ono što je nužno za legitimne i odobrene funkcije i aktivnosti te u tu svrhu uvode politike, postupke i kontrole koji se odnose na prava pristupa i osiguravaju dobro upravljanje njima;

(d) provode politike i protokole za pouzdane mehanizme autentifikacije, na temelju relevantnih standarda i namjenskih kontrolnih sustava, te mjere za zaštitu kriptografskih ključeva, kojima se podatci šifriraju na temelju rezultata odobrenih procesa klasifikacije podataka i procjene IKT rizika;

(e) provode dokumentirane politike, postupke i kontrole za upravljanje promjenama IKT-a, što uključuje promjene softvera, hardvera, komponenata ugrađenog softvera, sustava ili sigurnosnih parametara, koji se temelje na procjeni rizika i sastavni su dio općeg procesa upravljanja promjenama u financijskom subjektu, kako bi se osiguralo kontrolirano evidentiranje, testiranje, procjena, odobravanje, provedba i provjera svih promjena u IKT sustavima;

(f) posjeduju odgovarajuće i sveobuhvatne dokumentirane politike za zakrpe i ažuriranja.

Za potrebe prvog podstavka točke (b) financijski subjekti projektiraju infrastrukturu za mrežnu vezu tako da ju je moguće odmah prekinuti ili segmentirati kako bi se u najvećoj mogućoj mjeri smanjila i spriječila zaraza, posebno u slučaju međusobno povezanih financijskih procesa.

Za potrebe prvog podstavka točke (e) proces upravljanja promjenama IKT-a odobravaju odgovarajuće razine rukovodstva te on mora sadržavati posebne protokole.

Članak 10.

Otkrivanje

1. Financijski subjekti uspostavljaju mehanizme za brzo otkrivanje neobičnih aktivnosti, u skladu s člankom 17., što uključuje probleme s performansama IKT mreže i IKT incidente, te utvrđuju moguće bitne jedinstvene točke prekida.

Svi mehanizmi otkrivanja iz prvog podstavka redovito se testiraju u skladu s člankom 25.

2. Mehanizmima otkrivanja iz stavka 1. omogućuje se više razina kontrole, utvrđuju pragovi za upozorenja i kriteriji za aktiviranje i pokretanje procesâ odgovora na IKT incidente, što uključuje mehanizme za automatsko upozoravanje relevantnog osoblja zaduženog za odgovor na IKT incidente.

3. Financijski subjekti izdvajaju dostatne resurse i sposobnosti za praćenje aktivnosti korisnika, nastanka neobičnih pojava u IKT-u i IKT incidenata, posebno kibernapadâ.

4. Pružatelji usluga dostave podataka usto uspostavljaju sustave kojima se može djelotvorno provjeriti jesu li izvješća o trgovanju potpuna, kojima se mogu utvrditi propusti i očite pogreške te zahtijevati ponovni prijenos tih izvješća.

Članak 11.

Odgovor i oporavak

1. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. i na temelju zahtjevâ u pogledu utvrđivanja iz članka 8., financijski subjekti uvode sveobuhvatnu politiku kontinuiteta poslovanja u području IKT-a, koja se može donijeti kao zasebna namjenska politika koja je sastavni dio opće politike kontinuiteta poslovanja financijskog subjekta.

2. Financijski subjekti provode politiku kontinuiteta poslovanja u području IKT-a s pomoću namjenskih, primjerenih i dokumentiranih aranžmana, planova, postupaka i mehanizama čiji je cilj:

(a) osigurati kontinuitet ključnih ili važnih funkcija financijskog subjekta;

(b) brz, primjeren i djelotvoran odgovor na sve IKT incidente i njihovo rješavanje na način kojim se ograničava šteta, a prioritet daje nastavku poslovanja i mjerama oporavka;

(c) aktivirati, bez odgode, namjenske planove kojima se omogućuju mjere, procesi i tehnologije za suzbijanje širenja koji su prilagođeni svakoj vrsti IKT incidenta i sprečavanje daljnje štete, te prilagođene postupke odgovora i oporavka uspostavljene u skladu s člankom 12.;

(d) procijeniti preliminarne učinke, štete i gubitke;

(e) utvrditi komunikacijske mjere i mjere za upravljanje krizama kojima se osigurava prijenos ažuriranih informacija svim relevantnim članovima internog osoblja i vanjskim dionicima u skladu s člankom 14. te izvješćivanje nadležnih tijela u skladu s člankom 19.

3. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. financijski subjekti provode povezane planove odgovora i oporavka u području IKT-a, koji, kad je riječ o financijskim subjektima koji nisu mikropoduzeća, podliježu neovisnim unutarnjim revizijskim pregledima.

4. Financijski subjekti uvode, održavaju i periodički testiraju odgovarajuće planove kontinuiteta poslovanja u području IKT-a, prije svega za ključne ili važne funkcije koje su eksternalizirane ili ugovorene na temelju aranžmanâ s trećim stranama pružateljima IKT usluga.

5. U sklopu opće politike kontinuiteta poslovanja financijski subjekti provode analizu učinka na poslovanje (BIA) s obzirom na svoju izloženost ozbiljnim poremećajima u poslovanju. U okviru BIA-e financijski subjekti procjenjuju mogući učinak ozbiljnih poremećaja u poslovanju s pomoću kvantitativnih i kvalitativnih kriterija, pri čemu se služe unutarnjim i vanjskim podatcima i analizom scenarija, ovisno o potrebi. U okviru BIA-e razmatraju se ključnost utvrđenih i mapiranih poslovnih funkcija, potporni procesi, ovisnosti o trećim stranama i informacijske imovine, kao i njihove međuovisnosti. Financijski subjekti osiguravaju da se IKT imovina i IKT usluge oblikuju i upotrebljavaju u potpunosti u skladu s BIA-om, posebno kad je riječ o primjerenom osiguravanju redundantnosti svih ključnih komponenata.

6. U sklopu sveobuhvatnog upravljanja IKT rizicima financijski subjekti:

(a) testiraju planove kontinuiteta poslovanja u području IKT-a te planove odgovora i oporavka u području IKT-a u odnosu na IKT sustave kojima se podupiru sve funkcije, i to najmanje jedanput godišnje, kao i u slučaju svih bitnih promjena u IKT sustavima kojima se podupiru ključne ili važne funkcije;

(b) testiraju planove komunikacije u krizi izrađene u skladu s člankom 14.

Za potrebe prvog podstavka točke (a) financijski subjekti koji nisu mikropoduzeća u planove testiranja uključuju scenarije kibernapadâ i prebacivanja s primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i redundantnu infrastrukturu koji su potrebni za ispunjenje obveza utvrđenih u članku 12.

Financijski subjekti redovito preispituju svoju politiku kontinuiteta poslovanja u području IKT-a te svoje planove odgovora i oporavka u području IKT-a uzimajući u obzir rezultate testova provedenih u skladu s prvim podstavkom i preporuke iz revizijskih ili nadzornih provjera.

7. Financijski subjekti koji nisu mikropoduzeća imaju funkciju za upravljanje krizama kojom se, u slučaju aktivacije njihovih planova kontinuiteta poslovanja u području IKT-a ili njihovih planova odgovora i oporavka u području IKT-a, među ostalim utvrđuju jasni postupci za upravljanje unutarnjom i vanjskom komunikacijom u krizi u skladu s člankom 14.

8. U slučaju aktivacije planova kontinuiteta poslovanja u području IKT-a te planova odgovora i oporavka u području IKT-a, financijski subjekti vode evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna.

9. Središnji depozitoriji vrijednosnih papira nadležnim tijelima dostavljaju preslike rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi.

10. Financijski subjekti koji nisu mikropoduzeća nadležnim tijelima na zahtjev dostavljaju procjenu ukupnih godišnjih troškova i gubitaka prouzročenih značajnim IKT incidentima.

11. U skladu s člankom 16. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 europska nadzorna tijela u okviru zajedničkog odbora do 17. srpnja 2024. izrađuju zajedničke smjernice za procjenu ukupnih godišnjih troškova i gubitaka iz stavka 10.

Članak 12.

Politike i postupci za izradu sigurnosnih kopija te postupci i metode za ponovnu uspostavu i oporavak

1. Kako bi se osigurala ponovna uspostava IKT sustavâ i podataka uz minimalno razdoblje prekida rada te ograničene poremećaje u radu i gubitke, financijski subjekti u sklopu svojeg okvira za upravljanje IKT rizicima razvijaju i dokumentiraju:

(a) politike i postupke za izradu sigurnosnih kopija, u kojima se određuje opseg podataka za koje se izrađuju sigurnosne kopije te minimalna učestalost izrade sigurnosnih kopija, na temelju ključnosti informacija ili razine povjerljivosti podataka;

(b) postupke i metode za ponovnu uspostavu i oporavak.

2. Financijski subjekti uspostavljaju sustave za izradu sigurnosnih kopija, koji se mogu aktivirati u skladu s politikama i postupcima za izradu sigurnosnih kopija te postupcima i metodama za ponovnu uspostavu i oporavak. Aktivacijom sustavâ za izradu sigurnosnih kopija ne smije se ugroziti sigurnost mrežnih i informacijskih sustava ni dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka. Postupci za izradu sigurnosnih kopija te postupci i metode za ponovnu uspostavu i oporavak periodički se testiraju.

3. Pri vraćanju podataka sa sigurnosne kopije s pomoću vlastitih sustava financijski subjekti upotrebljavaju IKT sustave koji su fizički i logički odvojeni od izvornog IKT sustava. Ti IKT sustavi moraju biti zaštićeni od neovlaštenog pristupa ili oštećenja u području IKT-a te moraju omogućiti pravodobnu ponovnu uspostavu usluga, pri čemu se prema potrebi upotrebljavaju sigurnosne kopije podataka i sustava.

Središnjim drugim ugovornim stranama planovi oporavka omogućuju oporavak svih transakcija koje su bile u tijeku u trenutku poremećaja kako bi se omogućio siguran nastavak poslovanja središnje druge ugovorne strane te dovršila namira na zakazani datum.

Pružatelji usluga dostave podataka usto osiguravaju odgovarajuće resurse te imaju infrastrukturu za izradu sigurnosnih kopija i ponovnu uspostavu kako bi u svakom trenutku mogli nuditi i održati svoje usluge.

4. Financijski subjekti koji nisu mikropoduzeća održavaju redundantne IKT kapacitete opremljene resursima, sposobnostima i funkcijama koji su odgovarajući za pokrivanje poslovnih potreba. Mikropoduzeća na temelju svojeg profila rizičnosti procjenjuju potrebu za održavanjem takvih redundantnih IKT kapaciteta.

5. Središnji depozitoriji vrijednosnih papira održavaju najmanje jedno sekundarno mjesto obrade opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem za pokrivanje poslovnih potreba.

Sekundarno mjesto obrade:

(a) mora biti geografski udaljeno od primarnog mjesta obrade kako bi se osigurao drukčiji profil rizičnosti i kako bi se spriječilo da ga zahvati događaj koji je zahvatio primarno mjesto;

(b) mora moći osigurati kontinuitet ključnih ili važnih funkcija na isti način kao i primarno mjesto ili pružati razinu usluga koja je potrebna kako bi se osiguralo da financijski subjekt svoje ključne operacije obavi unutar ciljnih vrijednosti za oporavak;

(c) mora biti odmah dostupno osoblju financijskog subjekta kako bi se osigurao kontinuitet ključnih ili važnih funkcija u slučaju nedostupnosti primarnog mjesta obrade.

6. Pri utvrđivanju ciljeva kad je riječ o vremenu oporavka i točki oporavka za svaku funkciju financijski subjekti uzimaju u obzir radi li se o ključnoj ili važnoj funkciji te mogući opći učinak na učinkovitost tržišta. Tim ciljnim vremenima mora se osigurati da se u ekstremnim scenarijima postignu dogovorene razine usluga.

7. Pri oporavljanju od IKT incidenta financijski subjekti obavljaju potrebne provjere, uključujući višestruke provjere i usklađivanja, kako bi osigurali održavanje najviše razine cjelovitosti podataka. Te se provjere obavljaju i pri rekonstrukciji podataka vanjskih dionika kako bi se osigurala dosljednost podataka među sustavima.

Članak 13.

Učenje i razvoj

1. Financijski subjekti raspolažu sposobnostima i osobljem za prikupljanje informacija o ranjivostima i kiberprijetnjama, IKT incidentima, a osobito kibernapadima, te za analizu njihova vjerojatnog učinka na digitalnu operativnu otpornost financijskih subjekata.

2. Financijski subjekti uvode preispitivanja nakon IKT incidenata, koja se provode nakon što značajni IKT incidenti uzrokuju poremećaje u njihovim osnovnim aktivnostima, pri čemu analiziraju uzroke tih poremećaja i utvrđuju koja su poboljšanja potrebna za operacije IKT-a ili u okviru politike kontinuiteta poslovanja u području IKT-a iz članka 11.

Financijski subjekti koji nisu mikropoduzeća na zahtjev obavješćuju nadležna tijela o promjenama koje su provedene slijedom preispitivanja nakon IKT incidenata iz prvog podstavka.

U okviru preispitivanja nakon IKT incidenata iz prvog podstavaka utvrđuje se je li se postupalo u skladu s uspostavljenim postupcima te jesu li poduzete mjere bile djelotvorne, među ostalim i u pogledu:

(a) brzine odgovora na sigurnosna upozorenja i utvrđivanja učinka IKT incidenata i njihove ozbiljnosti;

(b) kvalitete i brzine provedbe forenzičke analize, u slučajevima u kojima se to smatra primjerenim;

(c) djelotvornosti eskalacije incidenta unutar financijskog subjekta;

(d) djelotvornosti unutarnje i vanjske komunikacije.

3. Pouke stečene iz testiranja digitalne operativne otpornosti provedenog u skladu s člancima 26. i 27. te iz stvarnih IKT incidenata, osobito kibernapadâ, kao i problemi koji se pojave po aktivaciji planova kontinuiteta poslovanja u području IKT-a te planova odgovora i oporavka u području IKT-a, zajedno s relevantnim informacijama razmijenjenima s partnerskim financijskim subjektima i procijenjenima tijekom nadzornih preispitivanja, propisno se i kontinuirano uključuju u proces procjene IKT rizikâ. Na temelju tih nalaza provode se odgovarajuća preispitivanja relevantnih komponenata okvira za upravljanje IKT rizicima iz članka 6. stavka 1.

4. Financijski subjekti prate djelotvornost provedbe svoje strategije za digitalnu operativnu otpornost iz članka 6. stavka 8. Financijski subjekti mapiraju kako se IKT rizici razvijaju s vremenom, analiziraju učestalost, vrste, razmjer i razvoj IKT incidenata, osobito kibernapadâ, te njihove obrasce, kako bi razumjeli razinu izloženosti IKT rizicima, osobito u odnosu na ključne ili važne funkcije, i poboljšali kiberzrelost i pripravnost konkretnog financijskog subjekta.

5. Više IKT osoblje najmanje jedanput godišnje izvješćuje upravljačko tijelo o nalazima iz stavka 3. te iznosi preporuke.

6. Financijski subjekti osmišljavaju programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti kao obvezne module u svojim programima osposobljavanja osoblja. Ti programi i osposobljavanja primjenjuju se na sve zaposlenike i više rukovodstvo, a razina njihove složenosti razmjerna je nadležnostima osoba koje obavljaju određene funkcije. Financijski subjekti u svoje relevantne programe osposobljavanja prema potrebi uključuju i treće strane pružatelje IKT usluga, u skladu s člankom 30. stavkom 2. točkom i.

7. Financijski subjekti koji nisu mikropoduzeća kontinuirano prate relevantna tehnološka dostignuća, također kako bi bolje razumjeli mogući učinak koji bi uvođenje tih novih tehnologija moglo imati na zahtjeve u pogledu sigurnosti IKT-a i digitalnu operativnu otpornost. Financijski subjekti koji nisu mikropoduzeća ostaju u toku s najnovijim procesima upravljanja IKT rizicima kako bi mogli djelotvorno suzbijati postojeće ili nove oblike kibernapada.

Članak 14.

Komunikacija

1. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. financijski subjekti izrađuju planove komunikacije u krizi, kojima se osigurava odgovorna objava barem značajnih IKT incidenata ili ranjivosti klijentima, partnerskim financijskim subjektima i javnosti, ovisno o slučaju.

2. U sklopu okvira za upravljanje IKT rizicima financijski subjekti provode komunikacijske politike za interno osoblje i vanjske dionike. U komunikacijskim politikama za osoblje uzima se u obzir potreba da se mora razlikovati osoblje uključeno u upravljanje IKT rizicima, posebno osoblje nadležno za odgovor i oporavak, od osoblja koje samo treba informirati.

3. Najmanje jedna osoba u financijskom subjektu zadužena je za provedbu komunikacijske strategije za IKT incidente i u tu svrhu ispunjava funkciju komunikacije s javnošću i medijima.

Članak 15.

Daljnje usklađivanje alata, metoda, procesa i politika za upravljanje IKT rizicima

Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s Agencijom Europske unije za kibersigurnost (ENISA), izrađuju zajednički nacrt regulatornih tehničkih standarda kako bi se:

(a) pobliže opisali elementi koje treba uključiti u politike, postupke, protokole i alate za sigurnost IKT-a iz članka 9. stavka 2. kako bi se osigurale sigurnost mreža i odgovarajuće mjere zaštite od neovlaštenih upada i zlouporabe podataka, očuvale dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka, što uključuje kriptografske tehnike, i zajamčio točan i brz prijenos podataka bez značajnih poremećaja i nepotrebnih zastoja;

(b) dodatno razradile komponente kontrole pravâ upravljanja pristupom iz članka 9. stavka 4. točke (c) i povezana politika ljudskih resursa, u okviru koje se pobliže opisuju prava pristupa, postupci za dodjelu i opoziv prava te praćenje neobičnog ponašanja u pogledu IKT rizika s pomoću odgovarajućih pokazatelja, među ostalim i za obrasce upotrebe mreže, sate, IT aktivnost i nepoznate uređaje;

(c) dodatno razradili mehanizmi utvrđeni u članku 10. stavku 1. koji omogućuju brzo otkrivanje neobičnih aktivnosti te kriteriji utvrđeni u članku 10. stavku 2. za aktiviranje otkrivanja IKT incidenata i procesa odgovora;

(d) pobliže opisale sastavnice politike kontinuiteta poslovanja u području IKT-a iz članka 11. stavka 1.;

(e) pobliže opisalo testiranje planova kontinuiteta poslovanja u području IKT-a iz članka 11. stavka 6. kako bi se osiguralo da se pri tom testiranju propisno uzimaju u obzir scenariji u kojima kvaliteta pružanja ključne ili važne funkcije opada do neprihvatljive razine ili pružanje te funkcije nije moguće te da se propisno razmatra mogući učinak nesolventnosti ili drugih oblika prekida relevantne treće strane pružatelja IKT usluga, kao i, ako je relevantno, politički rizici u jurisdikcijama u kojima ti pružatelji posluju;

(f) pobliže opisale sastavnice planova odgovora i oporavka u području IKT-a iz članka 11. stavka 3.;

(g) pobliže opisali sadržaj i format izvješća o preispitivanju okvira za upravljanje IKT rizicima iz članka 6. stavka 5.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja, uzimajući pritom u obzir sve posebne značajke koje proizlaze iz specifične prirode aktivnosti u različitim sektorima financijskih usluga.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. siječnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog stavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Članak 16.

Pojednostavljeni okvir za upravljanje IKT rizicima

1. Članci od 5. do 15. ove Uredbe ne primjenjuju se na mala i nepovezana investicijska društva, institucije za platni promet izuzete na temelju Direktive (EU) 2015/2366; institucije izuzete na temelju Direktive 2013/36/EU u odnosu na koje su države članice odlučile da neće primijeniti mogućnost iz članka 2. stavka 4. ove Uredbe; institucije za elektronički novac izuzete na temelju Direktive 2009/110/EZ; te male institucije za strukovno mirovinsko osiguranje.

Ne dovodeći u pitanje prvi podstavak, subjekti navedeni u prvom podstavku moraju:

(a) uspostaviti i održavati pouzdan i dokumentiran okvir za upravljanje IKT rizicima, u kojem se detaljno navode mehanizmi i mjere usmjereni na brzo, učinkovito i sveobuhvatno upravljanje IKT rizikom, među ostalim i za zaštitu relevantnih fizičkih komponenata i infrastrukture;

(b) kontinuirano pratiti sigurnost i funkcioniranje svih IKT sustava;

(c) učinak IKT rizika svesti na najmanju moguću mjeru s pomoću pouzdanih, otpornih i ažuriranih IKT sustava, protokola i alata koji su prikladni za potporu u obavljanju njihovih aktivnosti i pružanju usluga te kojima se na odgovarajući način štite dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka u mrežnim i informacijskim sustavima;

(d) omogućiti brzo utvrđivanje i otkrivanje izvora IKT rizika i neobičnih pojava u mrežnim i informacijskim sustavima te brzo postupanje u vezi s IKT incidentima;

(e) utvrditi ključne ovisnosti o trećim stranama pružateljima IKT usluga;

(f) osigurati kontinuitet ključnih ili važnih funkcija s pomoću planova kontinuiteta poslovanja te mjera odgovora i oporavka, koje uključuju barem mjere za izradu sigurnosnih kopija i ponovnu uspostavu;

(g) redovito testirati planove i mjere iz točke (f), kao i djelotvornost kontrola provedenih u skladu s točkama (a) i (c);

(h) u proces procjene IKT rizika prema potrebi uključiti relevantne operativne zaključke koji su rezultat testova iz točke (g) i analize nakon incidenata te razviti, u skladu s potrebama i profilom IKT rizičnosti, programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti za osoblje i rukovodstvo.

2. Okvir za upravljanje IKT rizicima iz stavka 1. drugog podstavka točke (a) dokumentira se i preispituje periodički, kao i po nastanku značajnih IKT incidenata, u skladu s uputama nadzornog tijela. Kontinuirano ga se poboljšava na temelju pouka koje proizlaze iz provedbe i praćenja. Izvješće o preispitivanju okvira za upravljanje IKT rizicima podnosi se nadležnom tijelu na njegov zahtjev.

3. Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s ENISA-om, izrađuju zajednički nacrt regulatornih tehničkih standarda kako bi se:

(a) pobliže opisali elementi koje treba uključiti u okvir za upravljanje IKT rizicima iz stavka 1. drugog podstavka točke (a);

(b) pobliže opisali elementi povezani sa sustavima, protokolima i alatima kojima se učinak IKT rizika iz stavka 1. drugog podstavka točke (c) svodi na najmanju moguću mjeru s ciljem osiguravanja sigurnosti mreža, omogućavanja odgovarajućih mjera zaštite od neovlaštenih upada i zlouporabe podataka te očuvanja dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka;

(c) pobliže opisale sastavnice planova kontinuiteta poslovanja u području IKT-a iz stavka 1. drugog podstavka točke (f);

(d) pobliže opisala pravila o testiranju planova kontinuiteta poslovanja i osigurala djelotvornost kontrola iz stavka 1. drugog podstavka točke (g), te osiguralo da se pri takvom testiranju propisno uzimaju u obzir scenariji u kojima kvaliteta pružanja ključne ili važne funkcije opada do neprihvatljive razine ili pružanje te funkcije nije moguće;

(e) pobliže opisali sadržaj i format izvješća o preispitivanju okvira za upravljanje IKT rizicima iz stavka 2.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. siječnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

POGLAVLJE III.

Upravljanje, klasifikacija i izvješćivanje u vezi s IKT incidentima

Članak 17.

Proces upravljanja IKT incidentima

1. Financijski subjekti definiraju, uspostavljaju i provode proces upravljanja IKT incidentima radi otkrivanja IKT incidenata, upravljanja njima i obavješćivanja o njima.

2. Financijski subjekti evidentiraju sve IKT incidente i ozbiljne kiberprijetnje. Financijski subjekti uspostavljaju odgovarajuće postupke i procese za osiguravanje dosljednog i integriranog praćenja IKT incidenata te postupanja i poduzimanja daljnjih mjera u vezi s njima kako bi se osiguralo utvrđivanje i dokumentiranje njihovih temeljnih uzroka te nošenje s tim uzrocima u cilju sprečavanja nastanka takvih incidenata.

3. U okviru procesa upravljanja IKT incidentima iz stavka 1.:

(a) uspostavljaju se pokazatelji za rano upozoravanje;

(b) uspostavljaju se postupci za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju IKT incidenata u skladu s njihovim prioritetom te ozbiljnosti i u skladu s ključnosti zahvaćenih usluga, u skladu s kriterijima utvrđenima u članku 18. stavku 1.;

(c) dodjeljuju se uloge i odgovornosti koje se moraju aktivirati za različite vrste IKT incidenata i scenarija;

(d) utvrđuju se planovi za komunikaciju s osobljem, vanjskim dionicima i medijima u skladu s člankom 14., planovi za obavješćivanje klijenata, za postupke povezane s internom eskalacijom, što uključuje prigovore korisnika povezane s IKT-om, te prema potrebi za informiranje partnerskih financijskih subjekata;

(e) osigurava se izvješćivanje relevantnog višeg rukovodstva barem o značajnim IKT incidentima te informiranje upravljačkog tijela barem o značajnim IKT incidentima, uz objašnjenje njihova učinka, odgovora na njih i dodatnih kontrola koje treba uvesti zbog takvih IKT incidenata;

(f) uspostavljaju se postupci odgovora na IKT incidente kako bi se ublažili njihovi učinci i osiguralo da usluge pravodobno postanu dostupne i sigurne.

Članak 18.

Klasifikacija IKT incidenata i kiberprijetnji

1. Financijski subjekti klasificiraju IKT incidente i utvrđuju njihov učinak na temelju sljedećih kriterija:

(a) broja i/ili relevantnosti zahvaćenih klijenata ili partnerskih financijskih subjekata i, ako je to primjenjivo, količine ili broja transakcija zahvaćenih IKT incidentom te činjenice je li IKT incident imao učinak na ugled financijskog subjekta;

(b) trajanja IKT incidenta, uključujući razdoblje prekida rada usluge;

(c) zemljopisne raširenosti u smislu područja koje je IKT incident zahvatio, osobito ako je zahvatio više od dvije države članice;

(d) gubitka podataka prouzročenog IKT incidentom, u smislu dostupnosti, vjerodostojnosti, cjelovitosti ili povjerljivosti podataka;

(e) ključnosti zahvaćenih usluga, uključujući transakcije i operacije financijskog subjekta;

(f) ekonomskog učinka IKT incidenta, što se prije svega odnosi na izravne i neizravne troškove i gubitke, i u apsolutnom i u relativnom smislu.

2. Financijski subjekti klasificiraju kiberprijetnje kao ozbiljne na temelju ključnosti usluga koje su izložene riziku, što uključuje transakcije i operacije financijskog subjekta, broj i/ili relevantnost zahvaćenih klijenata ili partnerskih financijskih subjekata i zemljopisnu raširenost područja izloženih riziku.

3. Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s ESB-om i ENISA-om, izrađuju zajednički nacrt regulatornih tehničkih standarda u kojem se pobliže opisuje sljedeće:

(a) kriteriji utvrđeni u stavku 1., uključujući pragove značajnosti za utvrđivanje značajnih IKT incidenata ili, ovisno o slučaju, značajnih operativnih ili sigurnosnih incidenata povezanih s plaćanjem koji su obuhvaćeni obvezom izvješćivanja utvrđenom u članku 19. stavku 1.;

(b) kriteriji koje nadležna tijela moraju primjenjivati u svrhu procjene relevantnosti značajnih IKT incidenata ili, ovisno o slučaju, značajnih operativnih ili sigurnosnih incidenata povezanih s plaćanjem, u odnosu na relevantna nadležna tijela u drugim državama članicama te pojedinosti izvješća o značajnim IKT incidentima ili, ovisno o slučaju, značajnim operativnim ili sigurnosnim incidentima povezanima s plaćanjem, koje se moraju podijeliti s ostalim nadležnim tijelima na temelju članka 19. stavaka 6. i 7.;

(c) kriteriji utvrđeni u stavku 2. ovog članka, uključujući visoke pragove značajnosti za utvrđivanje ozbiljnih kiberprijetnji.

4. Pri izradi zajedničkog nacrta regulatornih tehničkih standarda iz stavka 3. ovog članka europska nadzorna tijela uzimaju u obzir kriterije utvrđene u članku 4. stavku 2. te međunarodne standarde, smjernice i specifikacije koje izradi i objavi ENISA, uključujući prema potrebi specifikacije za druge gospodarske sektore. Za potrebe primjene kriterija utvrđenih u članku 4. stavku 2. europska nadzorna tijela propisno razmatraju potrebu da mikropoduzeća te mala i srednja poduzeća mobiliziraju dostatne resurse i kapacitete kako bi se osiguralo brzo upravljanje IKT incidentima.

Europska nadzorna tijela taj zajednički nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. siječnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz stavka 3. u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Članak 19.

Izvješćivanje o značajnim IKT incidentima i dobrovoljno obavješćivanje o ozbiljnim kiberprijetnjama

1. Financijski subjekti izvješćuju relevantna nadležna tijela iz članka 46. o značajnim IKT incidentima, u skladu sa stavkom 4. ovog članka.

Ako financijski subjekt podliježe nadzoru više nacionalnih nadležnih tijela iz članka 46., države članice imenuju jedno nadležno tijelo kao relevantno nadležno tijelo odgovorno za obavljanje funkcija i zadaća predviđenih u ovom članku.

Kreditne institucije koje su u skladu s člankom 6. stavkom 4. Uredbe (EU) br. 1024/2013 klasificirane kao značajne o značajnim IKT incidentima izvješćuju relevantno nacionalno nadležno tijelo imenovano u skladu s člankom 4. Direktive 2013/36/EU, koje to izvješće odmah prosljeđuje ESB-u.

Za potrebe prvog podstavka financijski subjekti, nakon što su prikupili i analizirali sve relevantne informacije, sastavljaju početnu obavijest i izvješća iz stavka 4. ovog članka s pomoću obrazaca iz članka 20. te ih dostavljaju nadležnom tijelu. Ako zbog tehničkih poteškoća nije moguće dostaviti početnu obavijest s pomoću obrasca, financijski subjekti obavješćuju nadležno tijelo o tome na neki drugi način.

Početna obavijest i izvješća iz stavka 4. sadržavaju sve informacije koje su nadležnom tijelu potrebne da bi utvrdilo ozbiljnost značajnog IKT incidenta i procijenilo moguće prekogranične učinke.

Ne dovodeći u pitanje izvješćivanje relevantnog nadležnog tijela od strane financijskog subjekta na temelju prvog podstavka, države članice povrh toga mogu odrediti da neki ili svi financijski subjekti početnu obavijest i svako izvješće iz stavka 4. ovog članka s pomoću obrazaca iz članka 20. također moraju dostaviti nadležnim tijelima ili timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovi) imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555.

2. Financijski subjekti mogu, na dobrovoljnoj osnovi, obavijestiti relevantno nadležno tijelo o ozbiljnim kiberprijetnjama ako smatraju da je prijetnja relevantna za financijski sustav, korisnike usluga ili klijente. Relevantno nadležno tijelo takve informacije može dostaviti drugim relevantnim tijelima iz stavka 6.

Kreditne institucije koje su klasificirane kao značajne u skladu s člankom 6. stavkom 4. Uredbe (EU) br. 1024/2013 mogu, na dobrovoljnoj osnovi, obavijestiti relevantno nacionalno nadležno tijelo imenovano u skladu s člankom 4. Direktive 2013/36/EU o ozbiljnim kiberprijetnjama, koje tu obavijest odmah prosljeđuje ESB-u.

Države članice mogu odrediti da oni financijski subjekti koji dostave obavijest na dobrovoljnoj osnovi u skladu s prvim podstavkom tu obavijest također mogu proslijediti CSIRT-ovima imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555.

3. Kad nastane značajan IKT incident koji utječe na financijske interese klijenata, financijski subjekti bez odgode, čim postanu svjesni tog incidenta, obavješćuju svoje klijente o tom značajnom IKT incidentu i o mjerama koje su poduzete kako bi se ublažili njegovi negativni učinci.

U slučaju ozbiljne kiberprijetnje financijski subjekti, ako je to primjenjivo, obavješćuju svoje klijente koji bi njome mogli biti zahvaćeni o svim odgovarajućim zaštitnim mjerama čije bi poduzimanje klijenti mogli razmotriti.

4. Financijski subjekti, u rokovima koje treba odrediti u skladu s člankom 20. prvim stavkom točkom (a) podtočkom ii, relevantnom nadležnom tijelu dostavljaju sljedeće:

(a) početnu obavijest;

(b) prijelazno izvješće nakon početne obavijesti iz točke (a) čim se status izvornog incidenta znatno promijeni ili se postupanje u vezi sa značajnim IKT incidentom promijeni na temelju novih dostupnih informacija, a nakon toga, prema potrebi, ažurirane obavijesti svaki put kad se pojave relevantne novosti o statusu kao i na izričit zahtjev nadležnog tijela;

(c) završno izvješće kad se dovrši analiza temeljnog uzroka incidenta, neovisno o tome jesu li mjere za ublažavanje učinka već provedene, i kad se procijenjene vrijednosti mogu zamijeniti stvarnim podatcima o učinku.

5. Financijski subjekti mogu, u skladu sa sektorskim pravom Unije i nacionalnim sektorskim pravom, eksternalizirati obveze izvješćivanja iz ovog članka trećoj strani pružatelju usluga. U slučaju takve eksternalizacije financijski subjekt ostaje u potpunosti odgovoran za ispunjavanje zahtjevâ u pogledu izvješćivanja o incidentima.

6. Nakon primitka početne obavijesti i svakog izvješća iz stavka 4. nadležno tijelo pravodobno dostavlja pojedinosti o značajnom IKT incidentu sljedećim primateljima, ovisno o tome u čijoj je nadležnosti dotični slučaj:

(a) EBA-i, ESMA-i ili EIOPA-i;

(b) ESB-u ako je riječ o financijskim subjektima iz članka 2. stavka 1. točaka (a), (b) i (d);

(c) nadležnim tijelima, jedinstvenim kontaktnim točkama ili CSIRT-ovima imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555;

(d) sanacijskim tijelima iz članka 3. Direktive 2014/59/EU i Jedinstvenom sanacijskom odboru (SRB) kad je riječ o subjektima iz članka 7. stavka 2. Uredbe (EU) br. 806/2014 Europskog parlamenta i Vijeća ([37]) te kad je riječ o subjektima i grupama iz članka 7. stavka 4. točke (b) i stavka 5. Uredbe (EU) br. 806/2014 ako se takve pojedinosti odnose na incidente koji predstavljaju rizik za osiguravanje ključnih funkcija u smislu članka 2. stavka 1. točke 35. Direktive 2014/59/EU; i

(e) drugim relevantnim tijelima javne vlasti u skladu s nacionalnim pravom.

7. Nakon što prime informacije u skladu sa stavkom 6., EBA, ESMA ili EIOPA i ESB, uz savjetovanje s ENISA-om i u suradnji s relevantnim nadležnim tijelom, procjenjuju je li dotični značajni IKT incident relevantan za nadležna tijela u drugim državama članicama. Nakon te procjene EBA, ESMA ili EIOPA u što kraćem roku obavješćuju relevantna nadležna tijela u drugim državama članicama. ESB obavješćuje članove Europskog sustava središnjih banaka o pitanjima koja su relevantna za platni sustav. Na temelju te obavijesti nadležna tijela prema potrebi poduzimaju sve potrebne mjere u svrhu zaštite neposredne stabilnosti financijskog sustava.

([37]) Uredba (EU) br. 806/2014 Europskog parlamenta i Vijeća od 15. srpnja 2014. o utvrđivanju jedinstvenih pravila i jedinstvenog postupka za sanaciju kreditnih institucija i određenih investicijskih društava u okviru jedinstvenog sanacijskog mehanizma i jedinstvenog fonda za sanaciju te o izmjeni Uredbe (EU) br. 1093/2010 (SL L 225, 30.7.2014., str. 1.).

8. Obavješću koju ESMA mora dostaviti na temelju stavka 7. ovog članka ne dovodi se u pitanje odgovornost nadležnog tijela da hitno prenese pojedinosti o značajnom IKT incidentu relevantnom tijelu u državi članici domaćinu ako središnji depozitorij vrijednosnih papira ima znatnu prekograničnu aktivnost u državi članici domaćinu, ako će značajni IKT incident vjerojatno imati ozbiljne posljedice za financijska tržišta države članice domaćina i ako među nadležnim tijelima postoje aranžmani za suradnju u vezi s nadzorom financijskih subjekata.

Članak 20.

Usklađivanje sadržaja i obrazaca izvješća

Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s ENISA-om i ESB-om, izrađuju:

(a) zajednički nacrt regulatornih tehničkih standarda u kojem se:

i. utvrđuje sadržaj izvješća o značajnim IKT incidentima kako bi se u obzir uzeli kriteriji iz članka 18. stavka 1. i uvrstili dodatni elementi, kao što su pojedinosti za određivanje jesu li izvješća relevantna za druge države članice i je li riječ o značajnom operativnom ili sigurnosnom incidentu povezanom s plaćanjem;

ii. određuju rokovi za početnu obavijest i za svako izvješće iz članka 19. stavka 4.;

iii. utvrđuje sadržaj obavijesti o ozbiljnim kiberprijetnjama.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja, posebno kako bi se osiguralo da se za potrebe točke (a) podtočke ii. ovog stavka različitim rokovima, ako je to primjereno, mogu uzeti u obzir posebnosti financijskih sektora, ne dovodeći u pitanje održavanje dosljednog pristupa izvješćivanju o IKT incidentima na temelju ove Uredbe i Direktive (EU) 2022/2555. Europska nadzorna tijela, ovisno o slučaju, dostavljaju obrazloženje kad odstupe od pristupa primijenjenih u kontekstu te direktive.

(b) zajednički nacrt provedbenih tehničkih standarda u kojem se utvrđuju standardni predlošci, obrasci i postupci za financijske subjekte za izvješćivanje o značajnim IKT incidentima i za obavješćivanje o ozbiljnoj kiberprijetnji.

Europska nadzorna tijela zajednički nacrt regulatornih tehničkih standarda iz prvog stavka točke (a) i zajednički nacrt provedbenih tehničkih standarda iz prvog stavka točke (b) dostavljaju Komisiji do 17. srpnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem zajedničkih regulatornih tehničkih standarda iz prvog stavka točke (a) u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Komisiji se dodjeljuje ovlast za donošenje zajedničkih provedbenih tehničkih standarda iz prvog stavka točke (b) u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Članak 21.

Centralizacija izvješćivanja o značajnim IKT incidentima

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i uz savjetovanje s ESB-om i ENISA-om, izrađuju zajedničko izvješće u kojem se procjenjuje izvedivost daljnje centralizacije izvješćivanja o incidentima uvođenjem jedinstvenog EU-ova centra za izvješćivanje o značajnim IKT incidentima za financijske subjekte. U tom zajedničkom izvješću istražuje se kako olakšati tijek izvješćivanja o IKT incidentima, smanjiti povezane troškove i poduprijeti tematske analize radi poboljšanja konvergencije nadzora.

2. Zajedničko izvješće iz stavka 1. sadržava barem sljedeće elemente:

(a) preduvjete za uvođenje jedinstvenog EU-ova centra;

(b) prednosti, ograničenja i rizike, uključujući rizike povezane s visokom koncentracijom osjetljivih informacija;

(c) potrebnu sposobnost za osiguravanje interoperabilnosti u odnosu na druge relevantne sustave izvješćivanja;

(d) elemente operativnog upravljanja;

(e) uvjete članstva;

(f) tehničke aranžmane za pristup financijskih subjekata i nacionalnih nadležnih tijela jedinstvenom EU-ovu centru;

(g) preliminarnu procjenu financijskih troškova koji bi nastali uspostavom operativne platforme koja bi podržavala jedinstveni EU-ov centar, što uključuje potrebno stručno znanje.

3. Europska nadzorna tijela izvješće iz stavka 1. dostavljaju Europskom parlamentu, Vijeću i Komisiji do 17. siječnja 2025.

Članak 22.

Povratne informacije o nadzoru

1. Ne dovodeći u pitanje tehničke doprinose, savjete ili korektivne mjere i daljnja postupanja koje, ako je to primjenjivo, u skladu s nacionalnim pravom pružaju i provode CSIRT-ovi iz Direktive (EU) 2022/2555, nadležno tijelo nakon primitka početne obavijesti i svakog izvješća iz članka 19. stavka 4. potvrđuje primitak i može, ako je to izvedivo, financijskom subjektu pravodobno dati relevantne i razmjerne povratne informacije ili smjernice na visokoj razini, posebno davanjem na uvid svih relevantnih anonimiziranih informacija i saznanja o sličnim prijetnjama, te može raspravljati o korektivnim mjerama koje su primijenjene na razini financijskog subjekta i o načinima za svođenje negativnih učinaka u cijelom financijskom sektoru na najmanju moguću mjeru i njihovo ublažavanje. Ne dovodeći u pitanje primljene povratne informacije o nadzoru, financijski subjekti snose potpunu odgovornost za postupanje u vezi s IKT incidentima o kojima je izviješćeno u skladu s člankom 19. stavkom 1. i za posljedice tih IKT incidenata.

2. Europska nadzorna tijela u okviru Zajedničkog odbora svake godine sastavljaju anonimizirano i agregirano izvješće o značajnim IKT incidentima, pri čemu pojedinosti o njima dostavljaju nadležna tijela u skladu s člankom 19. stavkom 6., u kojem se navode barem broj značajnih IKT incidenata, njihova priroda i učinak na poslovanje financijskih subjekata ili klijenata, poduzete korektivne mjere te nastali troškovi.

Europska nadzorna tijela izdaju upozorenja i izrađuju statistike na visokoj razini koje služe kao dopuna procjenama prijetnji i ranjivosti u području IKT-a.

Članak 23.

Operativni ili sigurnosni incidenti povezani s plaćanjem koji se odnose na kreditne institucije, institucije za platni promet, pružatelje usluga pružanja informacija o računu i institucije za elektronički novac

Zahtjevi utvrđeni u ovom poglavlju primjenjuju se i na operativne ili sigurnosne incidente povezane s plaćanjem te na značajne operativne ili sigurnosne incidente povezane s plaćanjem ako se oni odnose na kreditne institucije, institucije za platni promet, pružatelje usluga pružanja informacija o računu i institucije za elektronički novac.

POGLAVLJE IV.

Testiranje digitalne operativne otpornosti

Članak 24.

Opći zahtjevi za provedbu testiranja digitalne operativne otpornosti

1. Za potrebe procjene pripravnosti za postupanje u vezi s IKT incidentima, utvrđivanja slabosti, nedostataka i odstupanja u digitalnoj operativnoj otpornosti te brze provedbe korektivnih mjera financijski subjekti koji nisu mikropoduzeća, uzimajući u obzir kriterije utvrđene u članku 4. stavku 2., izrađuju, održavaju i preispituju pouzdan i sveobuhvatan program testiranja digitalne operativne otpornosti kao sastavni dio okvira za upravljanje IKT rizicima iz članka 6.

2. Program testiranja digitalne operativne otpornosti uključuje razne procjene, testove, metodologije, postupke i alate koji se moraju primjenjivati u skladu s člancima 25. i 26.

3. Kad provode programe testiranja digitalne operativne otpornosti iz stavka 1. ovog članka financijski subjekti koji nisu mikropoduzeća primjenjuju pristup koji se temelji na procjeni rizika, uzimajući u obzir kriterije utvrđene u članku 4. stavku 2., propisno vodeći računa o razvoju IKT rizika, konkretnim rizicima kojima je dotični financijski subjekt izložen ili bi mogao biti izložen, ključnosti informacijske imovine i usluga koje se pružaju te svim drugim čimbenicima koje financijski subjekt smatra primjerenima.

4. Financijski subjekti koji nisu mikropoduzeća osiguravaju da testove provode neovisne strane, unutarnje ili vanjske. Ako testove provodi unutarnji provoditelj testiranja, financijski subjekti namjenjuju dostatne resurse u tu svrhu i osiguravaju izbjegavanje sukoba interesa u fazama osmišljavanja i provedbe testa.

5. Financijski subjekti koji nisu mikropoduzeća uvode postupke i politike za određivanje prioriteta, klasifikaciju i ispravljanje svih problema otkrivenih tijekom testova te utvrđuju metodologije unutarnje provjere kako bi osigurali da se sve utvrđene slabosti, nedostatci ili odstupanja u potpunosti otklone.

6. Financijski subjekti koji nisu mikropoduzeća osiguravaju da se najmanje jedanput godišnje provedu primjereni testovi svih IKT sustava i aplikacija kojima se podupiru ključne ili važne funkcije.

Članak 25.

Testiranje IKT alata i sustava

1. Programom testiranja digitalne operativne otpornosti iz članka 24. predviđa se, u skladu s kriterijima utvrđenima u članku 4. stavku 2., provedba odgovarajućih testova, kao što su procjene i skeniranja ranjivosti, analize javno dostupnih izvora, procjene mrežne sigurnosti, analize odstupanja, preispitivanja fizičke sigurnosti, upitnici i softverska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvedivo, testiranja na temelju scenarija, testiranje kompatibilnosti, testiranje performansi, integralno testiranje (engl. *end-to-end testing*) i penetracijsko testiranje.

2. Središnji depozitoriji vrijednosnih papira i središnje druge ugovorne strane provode procjene ranjivosti prije svakog uvođenja ili ponovnog uvođenja novih ili postojećih aplikacija i infrastrukturnih komponenata te IKT usluga kojima se podupiru ključne ili važne funkcije financijskog subjekta.

3. Mikropoduzeća provode testove iz stavka 1. kombiniranjem pristupa koji se temelji na procjeni rizika sa strateškim planiranjem testiranja IKT-a, propisno uzimajući u obzir potrebu za održavanjem uravnoteženog pristupa između, s jedne strane, opsega resursa i vremena koje treba izdvojiti za testiranja IKT-a iz ovog članka i, s druge strane, hitnosti, vrste rizika, ključnosti informacijske imovine i usluga koje se pružaju te svih drugih relevantnih čimbenika, što uključuje sposobnost financijskog subjekta da preuzima promišljene rizike.

Članak 26.

Napredno testiranje IKT alata, sustava i procesa na temelju TLPT-a

1. Financijski subjekti koji nisu subjekti iz članka 16. stavka 1. prvog podstavka i koji nisu mikropoduzeća, koji su utvrđeni u skladu sa stavkom 8. trećim podstavkom ovog članka, provode napredno testiranje u obliku TLPT-a barem svake tri godine. Na temelju profila rizičnosti financijskog subjekta i uzimajući u obzir operativne okolnosti, nadležno tijelo prema potrebi može zatražiti od financijskog subjekta da tu učestalost smanji ili poveća.

2. Svaki penetracijski test vođen prijetnjama obuhvaća više ključnih ili važnih funkcija financijskog subjekta ili sve takve funkcije te se provodi na produkcijskim sustavima kojima se te funkcije podupiru.

Financijski subjekti utvrđuju sve relevantne temeljne IKT sustave, procese i tehnologije kojima se podupiru ključne ili važne funkcije te IKT usluge, među ostalim i one kojima se podupiru ključne ili važne funkcije koje su eksternalizirane ili ugovorene s trećim stranama pružateljima IKT usluga.

Financijski subjekti procjenjuju koje ključne ili važne funkcije moraju biti obuhvaćene TLPT-om. Na temelju rezultata te procjene određuje se točan opseg TLPT-a, a rezultate te procjene potvrđuju nadležna tijela.

3. Ako su treće strane pružatelji IKT usluga obuhvaćene TLPT-om, financijski subjekt poduzima potrebne mjere i zaštitne mjere kako bi osigurao sudjelovanje takvih trećih strana pružatelja IKT usluga u TLPT-u te u svakom trenutku zadržava potpunu odgovornost za osiguravanje usklađenosti s ovom Uredbom.

4. Ne dovodeći u pitanje stavak 2. prvi i drugi podstavak, ako se opravdano može očekivati da će sudjelovanje treće strane pružatelja IKT usluga u TLPT-u, kako je navedeno u stavku 3., negativno utjecati na kvalitetu ili sigurnost usluga koje treća strana pružatelj IKT usluga pruža klijentima koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe ili na povjerljivost podataka povezanih s takvim uslugama, financijski subjekt i treća strana pružatelj IKT usluga mogu se u pisanom obliku dogovoriti da treća strana pružatelj IKT usluga sklopi ugovorni aranžman izravno s vanjskim provoditeljem testiranja za potrebe provedbe, pod vodstvom jednog imenovanog financijskog subjekta, skupnog TLPT-a, u kojem sudjeluje više financijskih subjekata (skupno testiranje) kojima treća strana pružatelj IKT usluga pruža IKT usluge.

To skupno testiranje obuhvaća relevantan raspon IKT usluga kojima se podupiru ključne ili važne funkcije koje su financijski subjekti ugovorili s dotičnom trećom stranom pružateljem IKT usluga. Skupno testiranje smatra se TLPT-om koji provode financijski subjekti koji sudjeluju u skupnom testiranju.

Broj financijskih subjekata koji sudjeluju u skupnom testiranju na odgovarajući se način prilagođava uzimajući u obzir složenost i vrste usluga o kojima je riječ.

5. Financijski subjekti, u suradnji s trećim stranama pružateljima IKT usluga i ostalim uključenim stranama, uključujući provoditelje testiranja, ali ne i nadležna tijela, provode djelotvorne kontrole upravljanja rizicima kako bi ublažili rizike od mogućeg učinka na podatke, od oštećenja imovine i od poremećaja u radu ključnih ili važnih funkcija, usluga ili operacija u okviru samog financijskog subjekta, njegovih partnerskih financijskih subjekata ili u financijskom sektoru.

6. Na kraju testiranja, nakon što se postigne dogovor o izvješćima i planovima za ispravljanje nedostataka, financijski subjekt i, ako je to primjenjivo, vanjski provoditelji testiranja tijelu imenovanom u skladu sa stavkom 9. ili stavkom 10. dostavljaju sažetak relevantnih nalaza, planove za ispravljanje nedostataka i dokumentaciju kojom se potvrđuje da je TLPT proveden u skladu sa zahtjevima.

7. Tijela financijskim subjektima izdaju potvrdu da je test proveden u skladu sa zahtjevima, kako je potvrđeno u dokumentaciji, kako bi se omogućilo da nadležna tijela uzajamno priznaju penetracijske testove vođene prijetnjama. Financijski subjekt obavješćuje relevantno nadležno tijelo o potvrdi, sažetku relevantnih nalaza i planovima za ispravljanje nedostataka.

Ne dovodeći u pitanje takvu potvrdu, financijski subjekti u svakom trenutku snose punu odgovornost za učinke testova iz stavka 4.

8. Za potrebe provedbe TLPT-a financijski subjekti angažiraju provoditelje testiranja u skladu s člankom 27. Ako financijski subjekti za potrebe provedbe TLPT-a angažiraju unutarnje provoditelje testiranja, za svaki treći test dužni su angažirati vanjske provoditelje testiranja.

Kreditne institucije koje su klasificirane kao značajne u skladu s člankom 6. stavkom 4. Uredbe (EU) br. 1024/2013 angažiraju samo vanjske provoditelje testiranja, u skladu s člankom 27. stavkom 1. točkama od (a) do (e).

Nadležna tijela utvrđuju financijske subjekte koji su dužni provoditi TLPT, uzimajući u obzir kriterije utvrđene u članku 4. stavku 2., na temelju procjene sljedećeg:

(a) čimbenika povezanih s učinkom, posebno mjere u kojoj usluge koje financijski subjekt pruža i aktivnosti koje obavlja utječu na financijski sektor;

(b) mogućih problema u pogledu financijske stabilnosti, što uključuje sistemsku prirodu financijskog subjekta na razini Unije ili nacionalnoj razini, ovisno o slučaju;

(c) konkretnog profila IKT rizičnosti te stupnja IKT zrelosti financijskog subjekta ili tehnoloških značajki o kojima je riječ.

9. Države članice mogu imenovati jedinstveno tijelo javne vlasti u financijskom sektoru koje će biti odgovorno za pitanja povezana s TLPT-om u financijskom sektoru na nacionalnoj razini i tom tijelu povjeravaju sve nadležnosti i zadaće u vezi s time.

10. Ako se ne imenuje odgovarajuće jedinstveno tijelo javne vlasti u skladu sa stavkom 9. ovog članka, i ne dovodeći u pitanje ovlast za utvrđivanje financijskih subjekata koji su dužni provoditi TLPT, nadležno tijelo može delegirati izvršavanje nekih ili svih zadaća iz ovog članka i članka 27. nekom drugom nacionalnom tijelu u financijskom sektoru.

11. Europska nadzorna tijela, u dogovoru s ESB-om i u skladu s okvirom TIBER-EU, izrađuju zajednički nacrt regulatornih tehničkih standarda u kojem se pobliže opisuje sljedeće:

(a) kriteriji koji se primjenjuju za potrebe primjene stavka 8. drugog podstavka;

(b) zahtjevi i standardi koji se primjenjuju na angažiranje unutarnjih provoditelja testiranja;

(c) zahtjevi povezani s:

   i. opsegom TLPT-a iz stavka 2.;

   ii. metodologijom testiranja i pristupom koji treba primjenjivati u svakoj pojedinačnoj fazi testiranja;

   iii. rezultatima testiranja, završetkom testiranja i fazama testiranja koje se odnose na ispravljanje nedostataka;

(d) vrsta nadzorne suradnje i drugi relevantni oblici suradnje koji su potrebni za provedbu TLPT-a i za olakšavanje njegova uzajamnog priznavanja u kontekstu financijskih subjekata koji posluju u više država članica, kako bi se osigurala odgovarajuća razina uključenosti nadzornog tijela i fleksibilna provedba kojom se u obzir uzimaju posebnosti financijskih podsektora ili lokalnih financijskih tržišta.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela propisno uzimaju u obzir sve posebne značajke koje proizlaze iz specifične prirode aktivnosti u različitim sektorima financijskih usluga.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. srpnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Članak 27.

Zahtjevi za provoditelje testiranja u vezi s provedbom TLPT-a

1. Financijski subjekti za provedbu TLPT-a angažiraju samo provoditelje testiranja:

(a) koji su među najprikladnijim i najuglednijim provoditeljima testiranja;

(b) koji posjeduju tehničke i organizacijske sposobnosti i posebno stručno znanje u području saznanja o prijetnjama, penetracijskog testiranja i testiranja crvenog tima;

(c) koje je akreditiralo akreditacijsko tijelo u državi članici ili koji se pridržavaju formalnog kodeksa ponašanja ili etičkih okvira;

(d) koji daju neovisno jamstvo ili revizorsko izvješće u vezi s dobrim upravljanjem rizicima povezanima s provedbom TLPT-a, što uključuje odgovarajuću zaštitu povjerljivih informacija financijskog subjekta i pravnu zaštitu s obzirom na poslovne rizike financijskog subjekta;

(e) koji su propisno i u cijelosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, što uključuje rizike od protupravnog i nemarnog postupanja.

2. Kad angažiraju unutarnje provoditelja testiranja, financijski subjekti osiguravaju da su, uz zahtjeve iz stavka 1., ispunjeni i sljedeći zahtjevi:

(a) takvo angažiranje odobrilo je relevantno nadležno tijelo ili jedinstveno tijelo javne vlasti imenovano u skladu s člankom 26. stavcima 9. i 10.;

(b) relevantno nadležno tijelo potvrdilo je da financijski subjekt ima dostatne resurse i da je osigurao izbjegavanje sukoba interesa u fazama osmišljavanja i provedbe testa; i

(c) pružatelj saznanja o prijetnjama nije dio financijskog subjekta.

3. Financijski subjekti osiguravaju da se u ugovorima sklopljenima s vanjskim provoditeljima testiranja zahtijeva dobro upravljanje rezultatima TLPT-a i da ni jedna obrada podatka s tim u vezi, uključujući proizvodnju, pohranu, agregiranje, izradu, izvješćivanje, obavješćivanje ili uništavanje, ne stvara rizike za financijski subjekt.

POGLAVLJE V.

Upravljanje IKT rizikom povezanim s trećim stranama

Odjeljak I.

Ključna načela dobrog upravljanja IKT rizikom povezanim s trećim stranama

Članak 28.

Opća načela

1. Financijski subjekti upravljaju IKT rizikom povezanim s trećim stranama kao sastavnim dijelom IKT rizika u njihovu okviru za upravljanje IKT rizicima iz članka 6. stavka 1. i u skladu sa sljedećim načelima:

(a) financijski subjekti koji imaju sklopljene ugovorne aranžmane o upotrebi IKT usluga za potrebe svojeg poslovanja u svakom trenutku snose potpunu odgovornost za poštovanje i izvršavanje svih obveza iz ove Uredbe i primjenjivog prava o financijskim uslugama;

(b) financijski subjekti upravljaju IKT rizikom povezanim s trećim stranama poštujući načela proporcionalnosti i uzimajući u obzir:

i. prirodu, opseg, složenost i važnost ovisnosti u području IKT-a;

ii. rizike koji proizlaze iz ugovornih aranžmana o upotrebi IKT usluga sklopljenih s trećim stranama pružateljima IKT usluga, vodeći računa o ključnosti ili važnosti dotične usluge, procesa ili funkcije te o mogućem učinku na kontinuitet i dostupnost financijskih usluga i aktivnosti na razini subjekta i na razini grupe.

2. U sklopu svojih okvira za upravljanje IKT rizicima financijski subjekti koji nisu subjekti iz članka 16. stavka 1. prvog podstavka i koji nisu mikropoduzeća donose i redovito preispituju strategiju za IKT rizik povezan s trećim stranama, uzimajući u obzir, ako je to primjenjivo, strategiju nabave od više dobavljača iz članka 6. stavka 9. Strategija za IKT rizik povezan s trećim stranama obuhvaća politiku o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga, i primjenjuje se na pojedinačnoj i, prema potrebi, na potkonsolidiranoj i konsolidiranoj osnovi. Upravljačko tijelo na temelju procjene ukupnog profila rizičnosti financijskog subjekta te opsega i složenosti njegovih poslovnih usluga redovito preispituje rizike koji su utvrđeni u vezi s ugovornim aranžmanima o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije.

3. U sklopu okvira za upravljanje IKT rizicima financijski subjekti na razini subjekta te na potkonsolidiranoj i konsolidiranoj razini vode i ažuriraju registar informacija o svim ugovornim aranžmanima o upotrebi IKT usluga koje pružaju treće strane pružatelji IKT usluga.

Ugovorni aranžmani iz prvog podstavka na odgovarajući se način dokumentiraju tako da se aranžmani koji obuhvaćaju IKT usluge kojima se podupiru ključne ili važne funkcije razlikuju od onih koji ne obuhvaćaju takve usluge.

Financijski subjekti nadležna tijela najmanje jedanput godišnje izvješćuju o broju novih aranžmana o upotrebi IKT usluga, kategorijama trećih strana pružatelja IKT usluga, vrsti ugovornih aranžmana te o IKT uslugama i funkcijama koje se pružaju.

Financijski subjekti nadležnom tijelu na zahtjev stavljaju na raspolaganje cijeli registar informacija ili, ovisno o zahtjevu, njegove određene dijelove te sve informacije koje se smatraju potrebnima za djelotvoran nadzor nad financijskim subjektom.

Financijski subjekti pravodobno obavješćuju nadležno tijelo o svim planiranim ugovornim aranžmanima o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije te o tome da je određena funkcija postala ključna ili važna.

4. Prije sklapanja ugovornog aranžmana o upotrebi IKT usluga financijski subjekti:

(a) procjenjuju obuhvaća li ugovorni aranžman upotrebu IKT usluga kojima se podupire ključna ili važna funkcija;

(b) procjenjuju jesu li ispunjeni nadzorni uvjeti u pogledu ugovaranja;

(c) utvrđuju i procjenjuju sve relevantne rizike povezane s ugovornim aranžmanom, među ostalim i mogućnost da taj ugovorni aranžman doprinese jačanju koncentracijskog IKT rizika iz članka 29.;

(d) provode dubinske analize potencijalnih trećih strana pružatelja IKT usluga i osiguravaju prikladnost treće strane pružatelja IKT usluga tijekom cijelog procesa odabira i procesa procjene;

(e) utvrđuju i procjenjuju sukobe interesa koje bi ugovorni aranžman mogao izazvati.

5. Financijski subjekti mogu sklapati ugovorne aranžmane samo s trećim stranama pružateljima IKT usluga koje ispunjavaju odgovarajuće standarde informacijske sigurnosti. Kad se ti ugovorni aranžmani odnose na ključne ili važne funkcije, financijski subjekti prije njihova sklapanja propisno vode računa o tome da treće strane pružatelji IKT usluga primjenjuju najnovije i najkvalitetnije standarde informacijske sigurnosti.

6. Pri ostvarivanju pravâ na pristup, inspekcijski nadzor i reviziju u odnosu na treću stranu pružatelja IKT usluga financijski subjekti na temelju pristupa koji se temelji na procjeni rizika unaprijed utvrđuju učestalost revizija i inspekcijskog nadzora te područja u kojima treba provesti revizije, pridržavajući se općeprihvaćenih revizijskih standarda, u skladu s uputama nadzornog tijela o primjeni i uvrštenju tih revizijskih standarda.

Ako su ugovorni aranžmani sklopljeni s trećim stranama pružateljima IKT usluga o upotrebi IKT usluga tehnički vrlo složeni, financijski subjekt provjerava imaju li revizori, neovisno o tome je li riječ o unutarnjim ili vanjskim revizorima ili o skupini revizora, odgovarajuće vještine i znanje za djelotvornu provedbu relevantnih revizija i procjena.

7. Financijski subjekti osiguravaju mogućnost raskida ugovornog aranžmana o upotrebi IKT usluga u bilo kojoj od sljedećih situacija:

(a) treća strana pružatelj IKT usluga ozbiljno je prekršila primjenjive zakone, propise ili ugovorne uvjete;

(b) praćenjem IKT rizika povezanog s trećim stranama utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjena u izvršavanju funkcija koje se pružaju na temelju ugovornog aranžmana, što uključuje bitne promjene koje utječu na aranžman ili stanje treće strane pružatelja IKT usluga;

(c) treća strana pružatelj IKT usluga pokazala je slabosti u vezi s općim upravljanjem IKT rizicima, a posebno u načinu na koji osigurava dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka, bilo da je riječ o osobnim ili drugim osjetljivim podatcima ili pak neosobnim podatcima;

(d) nadležno tijelo zbog uvjeta dotičnog ugovornog aranžmana ili okolnosti povezanih s dotičnim ugovornim aranžmanom više ne može djelotvorno nadzirati financijski subjekt.

8. Kad je riječ o IKT uslugama kojima se podupiru ključne ili važne funkcije, financijski subjekti uvode izlazne strategije. U izlaznim strategijama uzimaju se u obzir rizici koji bi se mogli pojaviti na razini trećih strana pružatelja IKT usluga, osobito njihov mogući prekid, opadanje kvalitete IKT usluga koje se pružaju, poremećaji u poslovanju zbog neprikladnog ili neuspješnog pružanja IKT usluga ili svaki značajan rizik koji bi mogao nastati u vezi s prikladnošću i kontinuitetom uvođenja određene IKT usluge ili raskid ugovornog aranžmana s trećim stranama pružateljima IKT usluga u bilo kojoj od situacija navedenih u stavku 7.

Financijski subjekti osiguravaju da se mogu povući iz ugovornih aranžmana bez:

(a) remećenja svojih poslovnih aktivnosti;

(b) ograničavanja usklađenosti s regulatornim zahtjevima;

(c) narušavanja kontinuiteta i kvalitete usluga koje se pružaju klijentima.

Izlazni planovi moraju biti sveobuhvatni, dokumentirani i, u skladu s kriterijima utvrđenima u članku 4. stavku 2., moraju biti dostatno testirani te se moraju periodički preispitivati.

Financijski subjekti utvrđuju alternativna rješenja i izrađuju tranzicijske planove koji im omogućuju da se ugovorene IKT usluge te relevantni podatci od treće strane pružatelja IKT usluga sigurno i u cijelosti prenesu na alternativne pružatelje ili ponovno uključe u interni sustav.

Financijski subjekti uspostavljaju odgovarajuće mjere za nepredvidive situacije kako bi održali kontinuitet poslovanja ako dođe do okolnosti iz prvog podstavka.

9. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt provedbenih tehničkih standarda u kojem utvrđuju standardne obrasce za potrebe registra informacija iz stavka 3., što uključuje informacije koje se odnose na sve ugovorne aranžmane o upotrebi IKT usluga. Europska nadzorna tijela taj nacrt provedbenih tehničkih standarda dostavljaju Komisiji do 17. siječnja 2024.

Komisiji se dodjeljuje ovlast za donošenje provedbenih tehničkih standarda iz prvog podstavka u skladu s člankom 15. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

10. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt regulatornih tehničkih standarda u kojem pobliže opisuju detaljan sadržaj politike iz stavka 2. u pogledu ugovornih aranžmana o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja. Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. siječnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Članak 29.

Preliminarna procjena koncentracijskog IKT rizika na razini subjekta

1. Pri utvrđivanju i procjeni rizikâ iz članka 28. stavka 4. točke (c) financijski subjekti također uzimaju u obzir bi li predviđeno sklapanje ugovornog aranžmana o IKT uslugama kojima se podupiru ključne ili važne funkcije za posljedicu imalo bilo što od sljedećeg:

(a) ugovaranje usluga s trećom stranom pružateljem IKT usluga kojeg nije lako zamijeniti; ili

(b) više sklopljenih ugovornih aranžmana o pružanju IKT usluga kojima se podupiru ključne ili važne funkcije s istom trećom stranom pružateljem IKT usluga ili s usko povezanim trećim stranama pružateljima IKT usluga.

Financijski subjekti analiziraju koristi i troškove alternativnih rješenja, kao što je angažman različitih trećih strana pružatelja IKT usluga, uzimajući u obzir podudaraju li se predviđena rješenja s poslovnim potrebama i ciljevima utvrđenima u njihovoj strategiji digitalne otpornosti i u kojoj mjeri.

2. Ako je ugovornim aranžmanima o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije predviđena mogućnost da treća strana pružatelj IKT usluga može IKT usluge kojima se podupiru ključne ili važne funkcije podugovoriti nekoj drugoj trećoj strani pružatelju IKT usluga, financijski subjekti analiziraju potencijalne koristi i rizike tog podugovaranja, osobito ako podugovaratelj IKT usluga ima poslovni nastan u trećoj zemlji.

Ako se ugovorni aranžmani odnose na IKT usluge kojima se podupiru ključne ili važne funkcije, financijski subjekti propisno vode računa o odredbama prava o nesolventnosti koje bi se primjenjivale u slučaju stečaja treće strane pružatelja IKT usluga, kao i o svim ograničenjima do kojih bi moglo doći pri hitnom oporavku podataka financijskog subjekta.

Ako su ugovorni aranžmani o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije sklopljeni s trećom stranom pružateljem IKT usluga s poslovnim nastanom u trećoj zemlji, financijski subjekti, osim o elementima iz drugog podstavka, vode računa i o usklađenosti s pravilima Unije o zaštiti podataka te o djelotvornom izvršavanju zakonodavstva u toj trećoj zemlji.

Ako je u ugovornim aranžmanima o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije predviđeno podugovaranje, financijski subjekti procjenjuju mogu li, i u kojoj mjeri, potencijalno dugi ili složeni lanci podugovaranja utjecati na njihovu sposobnost da u potpunosti prate ugovorene funkcije i u tom smislu na sposobnost nadležnog tijela za djelotvoran nadzor nad financijskim subjektom.

Članak 30.

Ključne ugovorne odredbe

1. Prava i obveze financijskog subjekta i treće strane pružatelja IKT usluga jasno se dodjeljuju i utvrđuju u pisanom obliku. Cjeloviti ugovor uključuje sporazume o razini usluga te se navodi u jednom pisanom dokumentu koji je stranama dostupan u papirnatom obliku ili u dokumentu u nekom drugom trajnom i pristupačnom formatu koji se može preuzeti.

2. Ugovorni aranžmani o upotrebi IKT usluga sadržavaju barem sljedeće elemente:

(a) jasan i cjelovit opis svih funkcija i IKT usluga koje će pružati treća strana pružatelj IKT usluga, pri čemu se navodi je li dopušteno podugovaranje IKT usluge kojom se podupiru ključne ili važne funkcije ili njezinih bitnih dijelova te, ako jest, navode se i uvjeti koji se primjenjuju na takvo podugovaranje;

(b) lokacije, posebno regije ili zemlje, na kojima će se pružati ugovorene ili podugovorene funkcije i IKT usluge te na kojima će se obrađivati podatci, uključujući lokaciju pohrane, kao i zahtjev da treća strana pružatelj IKT usluga unaprijed obavijesti financijski subjekt ako namjerava promijeniti takve lokacije;

(c) odredbe o dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti u vezi sa zaštitom podataka, među ostalim i osobnih podataka;

(d) odredbe o osiguravanju pristupa osobnim i neosobnim podatcima koje obrađuje financijski subjekt te o osiguravanju njihova oporavka i vraćanja u lako dostupnom formatu u slučaju nesolventnosti, sanacije ili prestanka poslovanja treće strane pružatelja IKT usluga ili u slučaju raskida ugovornih aranžmana;

(e) opise razina usluga, uključujući ažuriranja i revizije tog opisa;

(f) obvezu treće strane pružatelja IKT usluga da pruži pomoć financijskom subjektu bez dodatnih troškova ili uz unaprijed utvrđene troškove u slučaju IKT incidenta koji je povezan s IKT uslugom koju ta treća strana pruža financijskom subjektu;

(g) obveza treće strane pružatelja IKT usluga da u potpunosti surađuje s nadležnim tijelima i sanacijskim tijelima financijskog subjekta, među ostalim i s osobama koje su ona imenovala;

(h) prava raskida i povezane minimalne rokove za prethodne obavijesti o raskidu ugovornih aranžmana u skladu s očekivanjima nadležnih tijela i sanacijskih tijela;

(i) uvjete za sudjelovanje trećih strana pružatelja IKT usluga u programima za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanjima o digitalnoj operativnoj otpornosti koje provode financijski subjekti u skladu s člankom 13. stavkom 6.

3. Ugovorni aranžmani o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, uz elemente iz stavka 2., sadržavaju barem sljedeće:

(a) potpune opise razina usluga, uključujući ažuriranja i revizije tog opisa, uz precizne kvantitativne i kvalitativne ciljeve uspješnosti u okviru dogovorenih razina usluga kako bi se financijskom subjektu omogućilo djelotvorno praćenje IKT usluga i poduzimanje, bez nepotrebne odgode, odgovarajućih korektivnih mjera ako se ne postignu dogovorene razine usluga;

(b) rokove za prethodne obavijesti i obveze izvješćivanja koje ima treća strana pružatelj IKT usluga u odnosu na financijski subjekt, uključujući obavijesti o svim događajima koji bi mogli bitno utjecati na sposobnost treće strane pružatelja IKT usluga za djelotvorno pružanje IKT usluga kojima se podupiru ključne ili važne funkcije u skladu s dogovorenim razinama usluga;

(c) zahtjeve da treća strana pružatelj IKT usluga uvede i testira planove za nepredvidive situacije u poslovanju te da uvede mjere, alate i politike za sigurnost IKT-a kojima se financijskom subjektu osigurava odgovarajuća razina sigurnosti za pružanje usluga, u skladu s njegovim regulatornim okvirom;

(d) obvezu treće strane pružatelja IKT usluga da sudjeluje u TLPT-u financijskog subjekta kako je navedeno u člancima 26. i 27. i da pritom bude u potpunosti kooperativna;

(e) pravo kontinuiranog praćenja rada treće strane pružatelja IKT usluga, što podrazumijeva sljedeće:

i. neograničena prava financijskog subjekta ili imenovane treće strane te nadležnog tijela na pristup, inspekcijski nadzor i reviziju te pravo na izradu preslika relevantne dokumentacije na licu mjesta ako je ključna za poslovanje treće strane pružatelja IKT usluga, pri čemu drugi ugovorni aranžmani ili provedbene politike ne sprečavaju i ne ograničavaju djelotvorno ostvarivanje tih prava;

ii. pravo ugovaranja alternativnih razina osiguranja ako su zahvaćena prava drugih klijenata;

iii. obvezu treće strane pružatelja IKT usluga da u potpunosti surađuje tijekom izravnih inspekcijskih nadzora i revizija koje provode nadležna tijela, glavno nadzorno tijelo, financijski subjekt ili imenovana treća strana;

iv. obvezu dostavljanja pojedinosti o opsegu, postupcima kojih se treba pridržavati i učestalosti takvih inspekcijskih nadzora i revizija;

(f) izlazne strategije, osobito određivanje obveznog primjerenog prijelaznog razdoblja:

i. tijekom kojega će treća strana pružatelj IKT usluga nastaviti pružati dotične funkcije ili IKT usluge kako bi se smanjio rizik od poremećaja u radu financijskog subjekta ili kako bi se osigurali njegova djelotvorna sanacija i restrukturiranje;

ii. u kojem financijski subjekt može prijeći na usluge druge treće strane pružatelja IKT usluga ili se prebaciti na interna rješenja, u skladu sa složenošću usluge koja se pruža.

Odstupajući od točke (e), treća strana pružatelj IKT usluga i financijski subjekt koji je mikropoduzeće mogu se dogovoriti da se prava financijskog subjekta u pogledu pristupa, inspekcijskog nadzora i revizije mogu delegirati neovisnoj trećoj strani, koju imenuje treća strana pružatelj IKT usluga, te da financijski subjekt može od te treće strane u bilo kojem trenutku zatražiti informacije i jamstvo o radu treće strane pružatelja IKT usluga.

4. Tijekom pregovora o ugovornim aranžmanima financijski subjekti i treće strane pružatelji IKT usluga dužni su razmotriti primjenu standardnih ugovornih klauzula koje su tijela javne vlasti sastavila za konkretne usluge.

5. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt regulatornih tehničkih standarda kojima se preciznije utvrđuju elementi iz stavka 2. točke (a) koje financijski subjekt treba utvrditi i procijeniti pri podugovaranju IKT usluga kojima se podupiru ključne ili važne funkcije.

Pri izradi tog nacrta regulatornih tehničkih standarda europska nadzorna tijela uzimaju u obzir veličinu i ukupni profil rizičnosti financijskog subjekta te prirodu, opseg i složenost njegovih usluga, aktivnosti i poslovanja.

Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. srpnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz prvog podstavka u skladu s člancima od 10. do 14. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010.

Odjeljak II.

Nadzorni okvir za ključne treće strane pružatelje IKT usluga

Članak 31.

Imenovanje ključnih trećih strana pružatelja IKT usluga

1. Europska nadzorna tijela u okviru Zajedničkog odbora i na preporuku Nadzornog foruma osnovanog na temelju članka 32. stavka 1.:

(a) imenuju treće strane pružatelje IKT usluga koji su ključni za financijske subjekte, nakon procjene kojom se uzimaju u obzir kriteriji navedeni u stavku 2.;

(b) imenuju glavnim nadzornim tijelom za svaku ključnu treću stranu pružatelja IKT usluga europsko nadzorno tijelo koje je, u skladu s uredbama (EU) br. 1093/2010, (EU) br. 1094/2010 ili (EU) br. 1095/2010, odgovorno za financijske subjekte koji zajedno imaju najveći udio ukupne imovine u vrijednosti ukupne imovine svih financijskih subjekata koji se koriste uslugama relevantne ključne treće strane pružatelja IKT usluga, što dokazuje zbroj pojedinačnih bilanci tih financijskih subjekata.

2. Imenovanje iz stavka 1. točke (a) temelji se na svim sljedećim kriterijima u vezi s IKT uslugama koje pruža treća strana pružatelj IKT usluga:

(a) sistemskom učinku na stabilnost, kontinuitet ili kvalitetu pružanja financijskih usluga u slučaju da se relevantna treća strana pružatelj IKT usluga suoči s prekidom većih razmjera u pružanju usluga, pri čemu se uzima u obzir broj financijskih subjekata i ukupna vrijednost imovine financijskih subjekata kojima relevantna treća strana pružatelj IKT usluga pruža usluge;

(b) sistemskoj prirodi ili značaju financijskih subjekata koji se oslanjaju na relevantnu treću stranu pružatelja IKT usluga, što se procjenjuje prema sljedećim parametrima:

i. broju globalnih sistemski važnih institucija (GSV institucije) ili drugih sistemski važnih institucija (OSV institucije) koje se oslanjanju na relevantnu treću stranu pružatelja IKT usluga;

ii. međuovisnosti GSV institucija ili OSV institucija iz podtočke i. i drugih financijskih subjekata, uključujući slučajeve u kojima GSV ili OSV institucije pružaju usluge financijske infrastrukture drugim financijskim subjektima;

(c) oslanjanju financijskih subjekata na usluge koje relevantna treća strana pružatelj IKT usluga pruža u vezi s ključnim ili važnim funkcijama financijskih subjekata u čije je pružanje u konačnici uključena ista treća strana pružatelj IKT usluga, neovisno o tome oslanjaju li se financijski subjekti na te usluge izravno ili neizravno, putem podugovornih aranžmana;

(d) stupnju zamjenjivosti treće strane pružatelja IKT usluga, uzimajući u obzir sljedeće parametre:

i. nepostojanje stvarnih alternativa, čak ni djelomičnih, zbog ograničenog broja trećih strana pružatelja IKT usluga koji su aktivni na određenom tržištu, ili tržišnog udjela relevantne treće strane pružatelja IKT usluga, ili relevantne tehničke složenosti ili sofisticiranosti, među ostalim i u pogledu zaštićene tehnologije, ili posebnosti organizacije ili aktivnosti treće strane pružatelja IKT usluga;

ii. poteškoće u vezi s djelomičnom ili potpunom migracijom relevantnih podataka i radnih opterećenja s relevantne treće strane pružatelja IKT usluga na drugu treću stranu pružatelja IKT usluga zbog znatnih financijskih troškova, vremena ili drugih resursa koji bi bili potrebni za migraciju ili zbog povećanog IKT rizika ili drugih operativnih rizika kojima bi financijski subjekt mogao biti izložen tijekom takve migracije;

3. Ako je treća strana pružatelj IKT usluga dio grupe, kriteriji iz stavka 2. razmatraju se u odnosu na IKT usluge koje pruža grupa kao cjelina.

4. Ključne treće strane pružatelji IKT usluga koje su dio grupe imenuju jednu pravnu osobu kao koordinacijsku točku kako bi se osigurali odgovarajuće zastupanje i komunikacija s glavnim nadzornim tijelom.

5. Glavno nadzorno tijelo obavješćuje treću stranu pružatelja IKT usluga o ishodu procjene koja je dovela do imenovanja iz stavka 1. točke (a). U roku od šest tjedana od datuma obavijesti treća strana pružatelj IKT usluga može glavnom nadzornom tijelu dostaviti obrazloženu izjavu sa svim relevantnim informacijama u svrhu procjene. Glavno nadzorno tijelo razmatra obrazloženu izjavu i može zatražiti da se u roku od 30 kalendarskih dana od primitka takve izjave dostave dodatne informacije.

Nakon što treću stranu pružatelja IKT usluga imenuju ključnom, europska nadzorna tijela u okviru Zajedničkog odbora obavješćuju treću stranu pružatelja IKT usluga o takvom imenovanju i početnom datumu od kojeg će efektivno podlijegati aktivnostima nadzora. Taj početni datum ne smije biti kasnije od mjesec dana nakon obavijesti. Treća strana pružatelj IKT usluga obavješćuje financijske subjekte kojima pruža usluge o tome da je imenovana kao ključna.

6. Komisija je ovlaštena za donošenje delegiranog akta u skladu s člankom 57. radi dopunjavanja ove Uredbe preciznijim utvrđivanjem kriterija iz stavka 2. ovog članka do 17. srpnja 2024.

7. Imenovanje iz stavka 1. točke (a) ne smije se primjenjivati dok Komisija ne donese delegirani akt u skladu sa stavkom 6.

8. Imenovanje iz stavka 1. točke (a) ne primjenjuje se na:

i. financijske subjekte koji pružaju IKT usluge drugim financijskim subjektima;

ii. treće strane pružatelje IKT usluga koje podliježu nadzornim okvirima uspostavljenima za potrebe podrške zadaćama iz članka 127. stavka 2. Ugovora o funkcioniranju Europske unije;

iii. pružatelje IKT usluga unutar grupe;

iv. treće strane pružatelje IKT usluga koje pružaju IKT usluge isključivo u jednoj državi članici financijskim subjektima koji posluju samo u toj državi članici.

9. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju, objavljuju i svake godine ažuriraju popis ključnih trećih strana pružatelja IKT usluga na razini Unije.

10. Za potrebe stavka 1. točke (a) nadležna tijela svake godine dostavljaju Nadzornom forumu osnovanom na temelju članka 32. agregirana izvješća iz članka 28. stavka 3. trećeg podstavka. Nadzorni forum procjenjuje ovisnost financijskih subjekata o IKT uslugama trećih strana na temelju informacija koje je dobio od nadležnih tijela.

11. Treće strane pružatelji IKT usluga koje nisu uvrštene na popis iz stavka 9. mogu zatražiti da ih se imenuje kao ključne u skladu sa stavkom 1. točkom (a).

Za potrebe prvog podstavka treća strana pružatelj IKT usluga dostavlja obrazložen zahtjev EBA-i, ESMA-i ili EIOPA-i, koje u okviru Zajedničkog odbora odlučuju hoće li tu treću stranu pružatelja IKT usluga imenovati kao ključnu u skladu sa stavkom 1. točkom (a).

Odluka iz drugog podstavka donosi se i o njoj se obavješćuje treću stranu pružatelja IKT usluga u roku od šest mjeseci od primitka zahtjeva.

12. Financijski subjekti smiju se koristiti uslugama treće strane pružatelja IKT usluga s poslovnim nastanom u trećoj zemlji koja je imenovana kao ključna u skladu sa stavkom 1. točkom (a) samo ako je ta treća strana osnovala društvo kćer u Uniji u roku od 12 mjeseci nakon imenovanja.

13. Ključna treća strana pružatelj IKT usluga iz stavka 12. obavješćuje glavno nadzorno tijelo o svim promjenama u strukturi uprave društva kćeri s poslovnim nastanom u Uniji.

Članak 32.

Struktura nadzornog okvira

1. U skladu s člankom 57. stavkom 1. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 Zajednički odbor osniva Nadzorni forum kao pododbor radi pružanja potpore radu Zajedničkog odbora i glavnog nadzornog tijela iz članka 31. stavka 1. točke (b) u području IKT rizika povezanog s trećim stranama u svim financijskim sektorima. Nadzorni forum izrađuje nacrt zajedničkih stajališta i nacrt zajedničkih akata Zajedničkog odbora u tom području.

Nadzorni forum redovito raspravlja o relevantnom razvoju u području IKT rizika i ranjivosti te na razini Unije promiče dosljedan pristup praćenju IKT rizika povezanog s trećim stranama.

2. Nadzorni forum svake godine provodi kolektivnu procjenu rezultata i nalaza aktivnosti nadzora provedenih nad svim ključnim trećim stranama pružateljima IKT usluga te promiče koordinacijske mjere radi povećanja digitalne operativne otpornosti financijskih subjekata, poticanja najboljih primjera iz prakse nošenja s koncentracijskim IKT rizikom i razmatranja instrumenata za smanjenje prijenosa rizika među sektorima.

3. Nadzorni forum predlaže sveobuhvatne referentne vrijednosti za ključne treće strane pružatelje IKT usluga koje Zajednički odbor donosi u obliku zajedničkih stajališta europskih nadzornih tijela u skladu s člankom 56. stavkom 1. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010.

4. Nadzorni forum čine:

(a) predsjednici europskih nadzornih tijela;

(b) po jedan predstavnik na visokoj razini iz svake države članice koji je član osoblja relevantnog nadležnog tijela iz članka 46.;

(c) izvršni direktori svih europskih nadzornih tijela i po jedan predstavnik Komisije, ESRB-a, ESB-a i ENISA-e kao promatrači;

(d) prema potrebi, po jedan dodatni predstavnik nadležnog tijela iz članka 46. iz svake države članice kao promatrač;

(e) ako je to primjenjivo, jedan predstavnik nadležnih tijela imenovanih ili uspostavljenih u skladu s Direktivom (EU) 2022/2555 koja su odgovorna za nadzor nad ključnim ili važnim subjektom koji podliježe toj direktivi, kojeg je ključna treća strana pružatelj IKT usluga imenovala kao promatrača.

Nadzorni forum može, prema potrebi, zatražiti savjet neovisnih stručnjaka imenovanih u skladu sa stavkom 6.

5. Svaka država članica imenuje relevantno nadležno tijelo čiji je član osoblja predstavnik na visokoj razini iz stavka 4. prvog podstavka točke (b) i o tome obavješćuje glavno nadzorno tijelo.

Europska nadzorna tijela na svojim internetskim stranicama objavljuju popis predstavnika na visokoj razini koje su imenovale države članice koji su članovi osoblja relevantnog nadležnog tijela.

6. Neovisne stručnjake iz stavka 4. drugog podstavka imenuje Nadzorni forum iz skupine stručnjaka odabranih nakon javnog i transparentnog natječajnog postupka.

Neovisni stručnjaci imenuju se na temelju njihova stručnog znanja u području financijske stabilnosti, digitalne operativne otpornosti i pitanja IKT sigurnosti. Oni djeluju neovisno i objektivno u isključivom interesu Unije kao cjeline, i ne traže niti primaju upute od institucija ili tijela Unije, bilo koje vlade države članice ili bilo kojeg drugog javnog ili privatnog tijela.

7. U skladu s člankom 16. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 europska nadzorna tijela do 17. srpnja 2024. izdaju, za potrebe ovog odjeljka, smjernice o suradnji između europskih nadzornih tijela i nadležnih tijela koje obuhvaćaju detaljne postupke i uvjete za raspodjelu i izvršavanje zadaća između nadležnih tijela i europskih nadzornih tijela te pojedinosti o razmjenama informacija koje su potrebne nadležnim tijelima kako bi se osiguralo daljnje postupanje prema preporukama na temelju članka 35. stavka 1. točke (d) koje su upućene ključnim trećim stranama pružateljima IKT usluga.

8. Zahtjevima utvrđenima u ovom odjeljku ne dovodi se u pitanje primjena Direktive (EU) 2022/2555 i drugih pravila Unije o nadzoru koja su primjenjiva na pružatelje usluga računalstva u oblaku.

9. Europska nadzorna tijela u okviru Zajedničkog odbora i na temelju pripremnog rada Nadzornog foruma jednom godišnje podnose izvješće o primjeni ovog odjeljka Europskom parlamentu, Vijeću i Komisiji.

Članak 33.

Zadaće glavnog nadzornog tijela

1. Glavno nadzorno tijelo, imenovano u skladu s člankom 31. stavkom 1. točkom (b), provodi nadzor nad ključnim trećim stranama pružateljima IKT usluga koje su mu dodijeljene i primarna je kontaktna točka za te ključne treće strana pružatelje IKT usluga u svrhu svih pitanja povezanih s nadzorom.

2. Za potrebe stavka 1. glavno nadzorno tijelo procjenjuje je li svaka ključna treća strana pružatelj IKT usluga uvela sveobuhvatna, pouzdana i djelotvorna pravila, postupke, mehanizme i aranžmane za upravljanje IKT rizicima kojima bi mogla izložiti financijske subjekte.

Procjena iz prvog podstavka uglavnom je usmjerena na IKT usluge koje pruža ključna treća strana pružatelj IKT usluga kojima se podupiru ključne ili važne funkcije financijskih subjekata. Ako je to potrebno za nošenje sa svim relevantnim rizicima, ta se procjena proširuje na IKT usluge kojima se podupiru funkcije koje nisu ključne ili važne.

3. Procjena iz stavka 2. obuhvaća:

(a) zahtjeve u području IKT-a kojima se osobito osiguravaju sigurnost, dostupnost, kontinuitet, skalabilnost i kvaliteta usluga koje ključna treća strana pružatelj IKT usluga pruža financijskim subjektima, kao i sposobnost da se u svakom trenutku zadrže visoki standardi dostupnosti, vjerodostojnosti, cjelovitosti ili povjerljivosti podataka;

(b) fizičku sigurnost koja doprinosi IKT sigurnosti, uključujući sigurnost prostora, objekata i podatkovnih centara;

(c) procese upravljanja rizicima, uključujući politike upravljanja IKT rizicima, politiku kontinuiteta poslovanja u području IKT-a te planove odgovora i oporavka u području IKT-a;

(d) aranžmane za upravljanje, uključujući organizacijsku strukturu s jasnim, transparentnim i dosljednim linijama odgovornosti te pravila o odgovornosti koja omogućuju djelotvorno upravljanje IKT rizicima;

(e) utvrđivanje i praćenje bitnih IKT incidenata te brzo izvješćivanje financijskih subjekata o njima, upravljanje tim incidentima, osobito kibernapadima, i njihovo rješavanje;

(f) mehanizme za prenosivost podataka, prenosivost aplikacija i interoperabilnost, kojima se financijskim subjektima osigurava djelotvorno ostvarivanje pravâ raskida;

(g) testiranje IKT sustava, infrastrukture i kontrola;

(h) revizije IKT-a;

(i) primjenu relevantnih nacionalnih i međunarodnih standarda koji su primjenjivi na pružanje IKT usluga financijskim subjektima.

4. Na temelju procjene iz stavka 2., i u koordinaciji sa Zajedničkom nadzornom mrežom iz članka 34. stavka 1., glavno nadzorno tijelo donosi jasan, detaljan i obrazložen pojedinačni plan nadzora u kojem se opisuju godišnji ciljevi nadzora i glavne mjere nadzora planirane za svaku ključnu treću stranu pružatelja IKT usluga. O tom se planu svake godine obavješćuje ključnu treću stranu pružatelja IKT usluga.

Prije donošenja plana nadzora glavno nadzorno tijelo dostavlja nacrt plana nadzora ključnoj trećoj strani pružatelju IKT usluga.

Nakon primitka nacrta plana nadzora ključna treća strana pružatelj IKT usluga može u roku od 15 kalendarskih dana dostaviti obrazloženu izjavu u kojoj dokazuje očekivani učinak na klijente koji nisu subjekti obuhvaćeni područjem primjene ove Uredbe i, prema potrebi, formulira rješenja za ublažavanje rizikâ.

5. Nakon što se donesu planovi nadzora iz stavka 4. i o njima se obavijeste ključne treće strane pružatelji IKT usluga, nadležna tijela mogu u pogledu tih ključnih trećih strana pružatelja IKT usluga poduzimati mjere samo u dogovoru s glavnim nadzornim tijelom.

Članak 34.

Operativna koordinacija između glavnih nadzornih tijela

1. Kako bi se osigurao dosljedan pristup aktivnostima nadzora i radi omogućivanja koordiniranih općih strategija nadzora i kohezivnih operativnih pristupa i metodologija rada, tri glavna nadzorna tijela imenovana u skladu s člankom 31. stavkom 1. točkom (b) uspostavljaju Zajedničku nadzornu mrežu radi međusobne koordinacije u pripremnim fazama i radi koordinacije provedbe aktivnosti nadzora nad nadziranim ključnim trećim stranama pružateljima IKT usluga, kao i tijekom svake mjere koja bi mogla biti potrebna u skladu s člankom 42.

2. Za potrebe stavka 1. glavna nadzorna tijela sastavljaju zajednički protokol nadzora kojim se utvrđuju detaljni postupci koje treba slijediti radi provedbe svakodnevne koordinacije i osiguravanja brzih razmjena i reakcija. Protokol se periodički revidira kako bi se njime uzele u obzir operativne potrebe, posebno razvoj praktičnih aranžmana za nadzor.

3. Glavna nadzorna tijela mogu, na ad hoc osnovi, pozvati ESB i ENISA-u da pruže tehničke savjete, podijele praktično iskustvo ili sudjeluju na posebnim koordinacijskim sastancima Zajedničke nadzorne mreže.

Članak 35.

Ovlasti glavnog nadzornog tijela

1. Za potrebe izvršavanja zadaća utvrđenih u ovom odjeljku glavno nadzorno tijelo u pogledu ključnih trećih strana pružatelja IKT usluga ovlašteno je:

(a) zahtijevati sve relevantne informacije i dokumentaciju u skladu s člankom 37.;

(b) provoditi opće istrage i inspekcijski nadzor u skladu s člankom 38. odnosno člankom 39.;

(c) nakon završetka aktivnosti nadzora zahtijevati izvješća u kojima se navode djelovanja ili korektivne mjere koje su ključne treće strane pružatelji IKT usluga poduzele ili provele u vezi s preporukama iz točke (d) ovog stavka;

(d) izdati preporuke u vezi s područjima iz članka 33. stavka 3., posebno o sljedećem:

i. primjeni posebnih zahtjeva ili procesa povezanih sa sigurnošću i kvalitetom IKT-a, osobito u pogledu uvođenja zakrpa, ažuriranja, enkripcije i drugih sigurnosnih mjera koje glavno nadzorno tijelo smatra važnima za IKT sigurnost usluga koje se pružaju financijskim subjektima;

ii. primjeni uvjeta, uključujući njihovu tehničku provedbu, pod kojima ključne treće strane pružatelji IKT usluga pružaju IKT usluge financijskim subjektima, a koje glavno nadzorno tijelo smatra važnima za sprečavanje nastanka jedinstvenih točaka prekida, njihova jačanja, ili za smanjenje, na najmanju moguću mjeru, mogućeg sistemskog učinka u cijelom financijskom sektoru Unije u slučaju koncentracijskog IKT rizika;

iii. svakom planiranom podugovaranju, ako glavno nadzorno tijelo na temelju provjere informacija prikupljenih u skladu s člancima 37. i 38. smatra da bi daljnje podugovaranje, uključujući podugovorne aranžmane koje ključna treća strana pružatelj IKT usluga planira sklopiti s trećim stranama pružateljima IKT usluga ili s podugovarateljima IKT usluga s poslovnim nastanom u trećoj zemlji, moglo izazvati rizike za usluge koje pruža financijski subjekt ili rizike za financijsku stabilnost;

iv. suzdržavanju od sklapanja daljnjih podugovornih aranžmana ako su ispunjeni sljedeći kumulativni uvjeti:

— predviđeni je podugovaratelj treća strana pružatelj IKT usluga ili podugovaratelj IKT usluga s poslovnim nastanom u trećoj zemlji;

— podugovaranje se odnosi na ključne ili važne funkcije financijskog subjekta; i

— glavno nadzorno tijelo smatra da primjena takvog podugovaranja predstavlja jasan i ozbiljan rizik za financijsku stabilnost Unije ili za financijske subjekte, što uključuje sposobnost financijskih subjekata da ispune zahtjeve u pogledu nadzora.

Za potrebe podtočke iv. ove točke treće strane pružatelji IKT usluga s pomoću predloška iz članka 41. stavka 1. točke (b) glavnom nadzornom tijelu dostavljanju informacije o podugovaranju.

2. Pri izvršavanju ovlasti iz ovog članka glavno nadzorno tijelo:

(a) osigurava redovitu koordinaciju u okviru Zajedničke nadzorne mreže, a posebno nastoji osigurati dosljedne pristupe, ako je to primjereno, kad je riječ o nadzoru nad ključnim trećim stranama pružateljima IKT usluga;

(b) propisno uzima u obzir okvir uspostavljen Direktivom (EU) 2022/2555 i, prema potrebi, savjetuje se s relevantnim nadležnim tijelima imenovanima ili uspostavljenima u skladu s tom direktivom kako bi se izbjeglo udvostručavanje tehničkih i organizacijskih mjera koje bi se mogle primjenjivati na ključne treće strane pružatelje IKT usluga na temelju te direktive;

(c) u mjeri u kojoj je to moguće, nastoji smanjiti rizik od poremećaja u uslugama koje ključne treće strane pružatelji IKT usluga pružaju klijentima koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe.

3. Glavno nadzorno tijelo savjetuje se s Nadzornim forumom prije izvršavanja ovlasti iz stavka 1.

Prije izdavanja preporuka u skladu sa stavkom 1. točkom (d) glavno nadzorno tijelo daje mogućnost trećoj strani pružatelju IKT usluga da u roku od 30 kalendarskih dana dostavi relevantne informacije kojima se dokazuje očekivani učinak na klijente koji su subjekti koji nisu obuhvaćeni područjem primjene ove Uredbe i, prema potrebi, oblikuju rješenja za ublažavanje rizikâ.

4. Glavno nadzorno tijelo obavješćuje Zajedničku nadzornu mrežu o ishodu izvršavanja ovlasti iz stavka 1. točaka (a) i (b). Glavno nadzorno tijelo bez nepotrebne odgode prosljeđuje izvješća iz stavka 1. točke (c) Zajedničkoj nadzornoj mreži i nadležnim tijelima financijskih subjekata koji se koriste IKT uslugama te ključne treće strane pružatelja IKT usluga.

5. Ključne treće strane pružatelji IKT usluga surađuju u dobroj vjeri s glavnim nadzornim tijelom i pomažu mu u obavljanju njegovih zadaća.

6. U slučaju potpune ili djelomične neusklađenosti s mjerama koje se moraju poduzeti u skladu s izvršavanjem ovlasti iz stavka 1. točaka (a), (b) i (c) i nakon isteka razdoblja od najmanje 30 kalendarskih dana od datuma kad je ključna treća strana pružatelj IKT usluga primila obavijest o dotičnim mjerama, glavno nadzorno tijelo donosi odluku kojom se izriče periodična novčana kazna kako bi se ključnu treću stranu pružatelja IKT usluga primoralo na poštovanje tih mjera.

7. Periodična novčana kazna iz stavka 6. izriče se na dnevnoj osnovi sve dok se ne osigura usklađenost i tijekom razdoblja od najviše šest mjeseci od obavijesti o odluci kojom se ključnoj trećoj strani pružatelju IKT usluga izriče periodična novčana kazna.

8. Iznos periodične novčane kazne, koji se izračunava od datuma utvrđenog u odluci kojom se izriče periodična novčana kazna, iznosi do 1 % prosječnoga dnevnog prometa na svjetskoj razini za ključnu treću stranu pružatelja IKT usluga u prethodnoj poslovnoj godini. Pri određivanju iznosa novčane kazne glavno nadzorno tijelo uzima u obzir sljedeće kriterije koji se odnose na neusklađenost s mjerama iz stavka 6.:

(a) ozbiljnost i trajanje neusklađenosti;

(b) je li neusklađenost počinjena namjerno ili iz nepažnje;

(c) razinu suradnje treće strane pružatelja IKT usluga s glavnim nadzornim tijelom.

Za potrebe prvog podstavka i kako bi se osigurao dosljedan pristup, glavno nadzorno tijelo sudjeluje u savjetovanju u okviru Zajedničke nadzorne mreže.

9. Novčane kazne administrativne su prirode i izvršive. Izvršenje se uređuje pravilima građanskog postupka koja su na snazi u državi članici na čijem se državnom području provodi inspekcijski nadzor i dodjeljuje pristup. Sudovi dotične države članice nadležni su za pritužbe koje se odnose na nepravilno izvršenje. Uplaćeni iznosi novčanih kazni dodjeljuju se u opći proračun Europske unije.

10. Glavno nadzorno tijelo javno objavljuje svaku izrečenu periodičnu novčanu kaznu, osim ako bi takva objava ozbiljno ugrozila financijska tržišta ili prouzročila nerazmjernu štetu uključenim stranama.

11. Prije izricanja periodične novčane kazne na temelju stavka 6. glavno nadzorno tijelo daje predstavnicima ključne treće strane pružatelja IKT usluga koja je predmet postupka mogućnost da se očituju o nalazima i svoje odluke temelji samo na nalazima o kojima se ključna treća strana pružatelj IKT usluga koja je predmet postupka mogla očitovati.

U postupku se u potpunosti poštuju prava na obranu osoba koje su predmet postupka. Ključna treća strana pružatelj IKT usluga koja je predmet postupka ima pravo na pristup spisu, pri čemu se mora uvažiti legitimni interes drugih osoba u pogledu zaštite njihovih poslovnih tajni. Pravo pristupa spisu ne odnosi se na povjerljive informacije ili interne pripremne dokumente glavnog nadzornog tijela.

Članak 36.

Izvršavanje ovlasti glavnog nadzornog tijela izvan Unije

1. Ako se ciljevi nadzora ne mogu postići interakcijom s društvom kćeri osnovanim za potrebe članka 31. stavka 12. ili obavljanjem aktivnosti nadzora u prostorima koji se nalaze u Uniji, glavno nadzorno tijelo može izvršavati ovlasti navedene u sljedećim odredbama, u svim prostorima koji se nalaze u trećoj zemlji i koji su u vlasništvu ključne treće strane pružatelja IKT usluga ili ih ona na bilo koji način upotrebljava za potrebe pružanja usluga financijskim subjektima u Uniji, a u vezi s njezinim poslovanjem, funkcijama ili uslugama, uključujući administrativne, poslovne ili operativne urede, prostore, zemljišta, zgrade ili druge nekretnine:

(a) članku 35. stavku 1. točki (a); i

(b) članku 35. stavku 1. točki (b), u skladu s člankom 38. stavkom 2. točkama (a), (b) i (d) te članku 39. stavku 1. i stavku 2. točki (a).

Ovlasti iz prvog podstavka mogu se izvršavati ako su ispunjeni svi sljedeći uvjeti:

i. glavno nadzorno tijelo smatra da je potrebno provesti inspekcijski nadzor u trećoj zemlji kako bi moglo u potpunosti i djelotvorno obaviti svoje zadaće na temelju ove Uredbe;

ii. inspekcijski nadzor u trećoj zemlji izravno je povezan s pružanjem IKT usluga financijskim subjektima u Uniji;

iii. dotična ključna treća strana pružatelj IKT usluga pristaje na provođenje inspekcijskog nadzora u trećoj zemlji; i

iv. glavno nadzorno tijelo službeno je obavijestilo relevantno tijelo dotične treće zemlje, koje protiv toga nije podnijelo prigovor.

2. Ne dovodeći u pitanje nadležnosti institucija Unije i država članica, za potrebe stavka 1. EBA, ESMA ili EIOPA sklapaju aranžmane za administrativnu suradnju s relevantnim tijelom treće zemlje kako bi glavno nadzorno tijelo i tim koji je ono odredilo za misiju u toj trećoj zemlji mogli neometano provoditi inspekcijski nadzor u dotičnoj trećoj zemlji. Tim aranžmanima za suradnju ne stvaraju se pravne obveze u odnosu na Uniju i njezine države članice niti se sprečava države članice i njihova nadležna tijela da sklapaju bilateralne ili multilateralne aranžmane s tim trećim zemljama i njihovim relevantnim tijelima.

Tim aranžmanima za suradnju utvrđuju se barem sljedeći elementi:

(a) postupci za koordinaciju aktivnosti nadzora koje se provode na temelju ove Uredbe i svako slično praćenje IKT rizika povezanog s trećim stranama u financijskom sektoru koje provodi relevantno tijelo dotične treće zemlje, uključujući pojedinosti o njegovu davanju suglasnosti kojom se glavnom nadzornom tijelu i timu koji je ono odredilo omogućuje da provode opće istrage i izravni inspekcijski nadzor iz stavka 1. prvog podstavka na državnom području pod njegovom nadležnošću;

(b) mehanizam za prenošenje svih relevantnih informacija između EBA-e, ESMA-e ili EIOPA-e i relevantnog tijela dotične treće zemlje, posebno u vezi s informacijama koje glavno nadzorno tijelo može zatražiti na temelju članka 37.;

(c) mehanizmi kojima relevantno tijelo dotične treće zemlje odmah obavješćuje EBA-u, ESMA-u ili EIOPA-u o slučajevima u kojima se smatra da je treća strana pružatelj IKT usluga s poslovnim nastanom u trećoj zemlji koja je u skladu s člankom 31. stavkom 1. točkom (a) imenovana kao ključna prekršila zahtjeve koje je na temelju mjerodavnog prava dotične treće zemlje obvezna poštovati pri pružanju usluga financijskim institucijama u toj trećoj zemlji, kao i o primijenjenim korektivnim mjerama i sankcijama;

(d) redovito prenošenje ažuriranih informacija o promjenama u području regulative i nadzora u vezi s praćenjem IKT rizika povezanog s trećim stranama za financijske institucije u dotičnoj trećoj zemlji;

(e) pojedinosti o omogućavanju sudjelovanja, ako je to potrebno, jednog predstavnika relevantnog tijela treće zemlje u inspekcijskom nadzoru koji provode glavno nadzorno tijelo i tim koji je ono odredilo.

3. Ako glavno nadzorno tijelo ne može provoditi aktivnosti nadzora iz stavaka 1. i 2. izvan Unije, ono:

(a) izvršava svoje ovlasti na temelju članka 35. na osnovi svih činjenica i dokumenata koji su mu dostupni;

(b) dokumentira i objašnjava sve posljedice svoje nemogućnosti provođenja predviđenih aktivnosti nadzora kako je navedeno u ovom članku.

Moguće posljedice iz točke (b) ovog stavka uzimaju se u obzir u preporukama glavnog nadzornog tijela izdanima na temelju članka 35. stavka 1. točke (d).

Članak 37.

Zahtjev za informacije

1. Glavno nadzorno tijelo može putem običnog zahtjeva ili odluke zatražiti da ključne treće strane pružatelji IKT usluga dostave sve informacije koje su glavnom nadzornom tijelu potrebne za izvršavanje njegovih zadaća na temelju ove Uredbe, uključujući sve relevantne poslovne ili operativne dokumente, ugovore, politike, dokumentaciju, izvješća o reviziji IKT sigurnosti, izvješća o IKT incidentima te sve informacije o stranama kojima je ključna treća strana pružatelj IKT usluga eksternalizirala operativne funkcije ili aktivnosti.

2. Pri slanju običnog zahtjeva za informacije iz stavka 1. glavno nadzorno tijelo:

(a) upućuje na ovaj članak kao pravnu osnovu za zahtjev;

(b) navodi svrhu zahtjeva;

(c) navodi koje se informacije traže;

(d) utvrđuje rok za dostavu informacija;

(e) obavješćuje predstavnika ključne treće strane pružatelja IKT usluga od koje se traže informacije da nije dužan dostaviti informacije, ali da u slučaju dobrovoljnog odgovora na zahtjev dostavljene informacije ne smiju biti netočne ili obmanjujuće.

3. Kad odlukom iz stavka 1. zahtijeva dostavu informacija, glavno nadzorno tijelo:

(a) upućuje na ovaj članak kao pravnu osnovu za zahtjev;

(b) navodi svrhu zahtjeva;

(c) navodi koje se informacije traže;

(d) utvrđuje rok za dostavu informacija;

(e) navodi periodične novčane kazne predviđene u članku 35. stavku 6. ako su dostavljene tražene informacije nepotpune ili ako takve informacije nisu dostavljene u roku iz točke (d) ovog stavka;

(f) upućuje na pravo na podnošenje žalbe protiv odluke Odboru za žalbe europskih nadzornih tijela i pravo na preispitivanje te odluke u postupku pred Sudom Europske unije („Sud”) u skladu s člancima 60. i 61. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010.

4. Predstavnici ključnih trećih strana pružatelja IKT usluga dostavljaju tražene informacije. Propisno ovlašteni odvjetnici mogu dostaviti informacije u ime svojih klijenata. Ključna treća strana pružatelj IKT usluga ostaje u potpunosti odgovorna ako su dostavljene informacije nepotpune, netočne ili obmanjujuće.

5. Glavno nadzorno tijelo nadležnim tijelima zaduženima za financijske subjekte koji se koriste uslugama dotične ključne treće strane pružatelja IKT usluga i Zajedničkoj nadzornoj mreži bez odgode dostavlja primjerak odluke kojom se zahtijeva dostava informacija.

Članak 38.

Opće istrage

1. Radi izvršavanja svojih zadaća na temelju ove Uredbe, glavno nadzorno tijelo uz pomoć zajedničkog tima za provjeru iz članka 40. stavka 1. može prema potrebi provoditi istrage ključnih trećih strana pružatelja IKT usluga.

2. Glavno nadzorno tijelo ovlašteno je:

(a) pregledavati evidenciju, podatke, postupke i sve ostale materijale relevantne za obavljanje svojih zadaća, neovisno o tome na kojem su mediju pohranjeni;

(b) izraditi ili pribaviti ovjerene preslike ili izvatke iz te evidencije, podataka, dokumentiranih postupaka i svih ostalih materijala;

(c) pozvati predstavnike ključne treće strane pružatelja IKT usluga da daju usmena ili pisana objašnjenja o činjenicama ili dokumente koji se odnose na predmet i svrhu istrage te zabilježiti odgovore;

(d) obaviti razgovor sa svakom fizičkom ili pravnom osobom koja pristane na razgovor radi prikupljanja informacija koje se odnose na predmet istrage;

(e) zatražiti evidenciju telefonskih razgovora i podatkovnog prometa.

3. Službenici i druge osobe koje glavno nadzorno tijelo ovlasti za potrebe istrage iz stavka 1. izvršavaju svoje ovlasti uz predočenje pisanog ovlaštenja u kojem se navode predmet i svrha istrage.

U tom se ovlaštenju navode i periodične novčane kazne predviđene u članku 35. stavku 6. ako tražena evidencija, podatci, dokumentirani postupci ili bilo koji drugi materijal ili odgovori na pitanja postavljena predstavnicima treće strane pružatelja IKT usluga nisu dostavljeni ili su nepotpuni.

4. Predstavnici ključnih trećih strana pružatelja IKT usluga moraju pristati na istrage koje se pokrenu na temelju odluke glavnog nadzornog tijela. U odluci se navode predmet i svrha istrage, periodične novčane kazne predviđene u članku 35. stavku 6., pravni lijekovi dostupni na temelju uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010 te pravo na preispitivanje odluke pred Sudom.

5. Pravodobno prije početka istrage glavno nadzorno tijelo obavješćuje nadležna tijela zadužena za financijske subjekte koji se koriste IKT uslugama te ključne treće strane pružatelja IKT usluga o predviđenoj istrazi i identitetu ovlaštenih osoba.

Glavno nadzorno tijelo dostavlja Zajedničkoj nadzornoj mreži sve informacije primljene na temelju prvog podstavka.

Članak 39.

Inspekcijski nadzor

1. Radi izvršavanja svojih zadaća na temelju ove Uredbe glavno nadzorno tijelo uz pomoć zajedničkih timova za provjeru iz članka 40. stavka 1. može ulaziti u sve poslovne prostore, na zemljišta ili u nekretnine trećih strana pružatelja IKT usluga, kao što su registrirana sjedišta, operativni centri, sekundarni poslovni prostori, i u njima provoditi sav potreban izravni, ali i neizravni inspekcijski nadzor.

Za potrebe izvršavanja ovlasti iz prvog podstavka glavno nadzorno tijelo savjetuje se sa Zajedničkom nadzornom mrežom.

2. Službenici i druge osobe koje je glavno nadzorno tijelo ovlastilo za provođenje izravnog inspekcijskog nadzora ovlaštene su:

(a) ulaziti u sve takve poslovne prostore, na zemljišta ili u nekretnine; i

(b) zapečatiti sve takve poslovne prostore, knjige ili evidenciju, tijekom inspekcijskog nadzora i u mjeri u kojoj je to potrebno za inspekcijski nadzor.

Službenici i druge osobe koje je ovlastilo glavno nadzorno tijelo izvršavaju svoje ovlasti uz predočenje pisanog ovlaštenja u kojem se navode predmet i svrha inspekcijskog nadzora te periodične novčane kazne predviđene u članku 35. stavku 6. ako predstavnici dotične ključne treće strane pružatelja IKT usluga ne pristanu na inspekcijski nadzor.

3. Pravodobno prije početka inspekcijskog nadzora glavno nadzorno tijelo o tome obavješćuje nadležna tijela zadužena za financijske subjekte koji se koriste uslugama te treće strane pružatelja IKT usluga.

4. Inspekcijski nadzor obuhvaća cijeli dijapazon relevantnih IKT sustava, mreže, uređaje, informacije i podatke koji se koriste za pružanje IKT usluga financijskim subjektima ili mu doprinose.

5. Prije planiranog izravnog inspekcijskog nadzora glavno nadzorno tijelo u razumnom roku o tome obavješćuje ključne treće strane pružatelje IKT usluga, osim ako slanje obavijesti u tom roku nije moguće zbog hitne ili krizne situacije ili ako bi slanje obavijesti dovelo do situacije u kojoj inspekcijski nadzor ili revizija više ne bi bili djelotvorni.

6. Ključna treća strana pružatelj IKT usluga mora pristati na izravni inspekcijski nadzor naložen odlukom glavnog nadzornog tijela. U odluci se navode predmet i svrha inspekcijskog nadzora, određuje datum početka inspekcijskog nadzora te se navode periodične novčane kazne predviđene u članku 35. stavku 6., pravni lijekovi dostupni na temelju uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010, kao i pravo na preispitivanje odluke pred Sudom.

7. Ako službenici i druge osobe koje je ovlastilo glavno nadzorno tijelo utvrde da se ključna treća strana pružatelj IKT usluga protivi inspekcijskom nadzoru naloženom na temelju ovog članka, glavno nadzorno tijelo obavješćuje ključnu treću stranu pružatelja IKT usluga o posljedicama takvog protivljenja, među ostalim i o mogućnosti da nadležna tijela zadužena za relevantne financijske subjekte od financijskih subjekata zatraže da raskinu ugovorne aranžmane sklopljene s tom ključnom trećom stranom pružateljem IKT usluga.

Članak 40.

Kontinuirani nadzor

1. U provedbi aktivnosti nadzora, osobito općih istraga ili inspekcijskog nadzora, glavnom nadzornom tijelu pomaže zajednički tim za provjeru koji se osniva za svaku ključnu treću stranu pružatelja IKT usluga.

2. Zajednički tim za provjeru iz stavka 1. čine članovi osoblja iz:

(a) europskih nadzornih tijela;

(b) relevantnih nadležnih tijela koja nadziru financijske subjekte kojima ključna treća strana pružatelj IKT usluga pruža IKT usluge;

(c) nacionalnog nadležnog tijela iz članka 32. stavka 4. točke (e), na dobrovoljnoj osnovi;

(d) jednog nacionalnog nadležnog tijela iz države članice u kojoj ključna treća strana pružatelj IKT usluga ima poslovni nastan, na dobrovoljnoj osnovi.

Članovi zajedničkog tima za provjeru moraju imati stručno znanje iz područja IKT-a i operativnih rizika. Rad zajedničkog tima za provjeru koordinira član osoblja glavnog nadzornog tijela koji se za to odredi („koordinator glavnog nadzornog tijela”).

3. U roku od tri mjeseca od završetka istrage ili inspekcijskog nadzora, a nakon savjetovanja s Nadzornim forumom, glavno nadzorno tijelo donosi preporuke koje upućuje ključnoj trećoj strani pružatelju IKT usluga na temelju svojih ovlasti iz članka 35.

4. Preporuke iz stavka 3. odmah se dostavljaju ključnoj trećoj strani pružatelju IKT usluga i nadležnim tijelima zaduženima za financijske subjekte kojima ona pruža IKT usluge.

Za potrebe izvršavanja aktivnosti nadzora glavno nadzorno tijelo može uzeti u obzir sve relevantne certifikate treće strane i izvješća unutarnjih ili vanjskih revizora o trećoj strani pružatelju IKT usluga koje im na raspolaganje stavi ključna treća strana pružatelj IKT usluga.

Članak 41.

Usklađivanje uvjeta koji omogućuju provedbu aktivnosti nadzora

1. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt regulatornih tehničkih standarda kako bi pobliže opisala:

(a) informacije koje treća strana pružatelj IKT usluga mora dostaviti u dobrovoljno upućenom zahtjevu da je se u skladu s člankom 31. stavkom 11. imenuje kao ključnu;

(b) sadržaj, strukturu i format informacija koje moraju dostaviti, objaviti ili o kojima moraju izvijestiti treće strane pružatelji IKT usluga na temelju članka 35. stavka 1., uključujući predložak za dostavljanje informacija o podugovornim aranžmanima;

(c) kriterije za utvrđivanje sastava zajedničkog tima za provjeru kojima se osigurava uravnoteženo sudjelovanje članova osoblja europskih nadzornih tijela i osoblja relevantnih nadležnih tijela, te za utvrđivanje njihova imenovanja, zadaća i načina rada;

(d) pojedinosti o procjeni nadležnih tijela u pogledu mjera koje je ključna treća strana pružatelj IKT usluga poduzela na osnovi preporuka glavnog nadzornog tijela na temelju članka 42. stavka 3.

2. Europska nadzorna tijela taj nacrt regulatornih tehničkih standarda dostavljaju Komisiji do 17. srpnja 2024.

Komisiji se dodjeljuje ovlast za dopunjavanje ove Uredbe donošenjem regulatornih tehničkih standarda iz stavka 1. u skladu s postupkom utvrđenim u člancima od 10. do 14. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010.

Članak 42.

Daljnje mjere nadležnih tijela

1. U roku od 60 kalendarskih dana od primitka preporuka koje je glavno nadzorno tijelo izdalo na temelju članka 35. stavka 1. točke (d) ključne treće strane pružatelji IKT usluga ili obavješćuju glavno nadzorno tijelo o svojoj namjeri da slijede preporuke ili dostavljaju obrazloženo objašnjenje u kojem navode zašto neće slijediti te preporuke. Glavno nadzorno tijelo odmah te informacije prosljeđuju nadležnim tijelima zaduženima za dotične financijske subjekte.

2. Glavno nadzorno tijelo javno obavješćuje o slučajevima u kojima ga ključna treća strana pružatelj IKT usluga ne obavijesti u skladu sa stavkom 1. ili u kojima se objašnjenje koje je dostavila ključna treća strana pružatelj IKT usluga ne smatra dostatnim. U objavljenim informacijama otkriva se identitet ključne treće strane pružatelja IKT usluga te se navode informacije o vrsti i prirodi neusklađenosti. Takve su informacije ograničene na ono što je relevantno i razmjerno u svrhu osiguravanja javne osviještenosti, osim ako bi takvo objavljivanje uzrokovalo nerazmjernu štetu uključenim stranama ili bi moglo ozbiljno ugroziti uredno funkcioniranje i cjelovitost financijskih tržišta ili stabilnost cijelog financijskog sustava Unije ili njegova dijela.

Glavno nadzorno tijelo obavješćuje treću stranu pružatelja IKT usluga o toj objavi.

3. Nadležna tijela obavješćuju relevantne financijske subjekte o rizicima utvrđenima u preporukama upućenima ključnim trećim stranama pružateljima IKT usluga u skladu s člankom 35. stavkom 1. točkom (d).

Pri upravljanju IKT rizikom povezanim s trećim stranama financijski subjekti uzimaju u obzir rizike navedene u prvom podstavku.

4. Ako nadležno tijelo smatra da financijski subjekt u okviru svojeg upravljanja IKT rizikom povezanim s trećim stranama ne uzima u obzir konkretne rizike utvrđene u preporukama ili se u dostatnoj mjeri ne nosi s tim rizicima, ono obavješćuje financijski subjekt o mogućnosti da u roku od 60 kalendarskih dana od primitka takve obavijesti, ako ne postoje odgovarajući ugovorni aranžmani čiji je cilj nošenje s takvim rizicima, donese odluku na temelju stavka 6.

5. Nakon primitka izvješća iz članka 35. stavka 1. točke (c) i prije donošenja odluke iz stavka 6. ovog članka nadležna tijela mogu se na dobrovoljnoj osnovi savjetovati s nadležnim tijelima imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555 koja su odgovorna za nadzor nad ključnim ili važnim subjektom koji podliježe toj direktivi i koji je imenovan ključnom trećom stranom pružateljem IKT usluga.

6. Nadležna tijela, kao krajnju mjeru nakon obavijesti i, ako je to primjereno, nakon savjetovanja iz stavaka 4. i 5. ovog članka, mogu u skladu s člankom 50. donijeti odluku kojom se od financijskih subjekata zahtijeva da djelomično ili u cijelosti privremeno suspendiraju korištenje ili uvođenje usluge koju im pruža ključna treća strana pružatelj IKT usluga dok se ne uklone rizici utvrđeni u preporukama upućenima ključnim trećim stranama pružateljima IKT usluga. Prema potrebi, nadležna tijela mogu od financijskih subjekata zatražiti da raskinu, djelomično ili u cijelosti, relevantne ugovorne aranžmane sklopljene s ključnim trećim stranama pružateljima IKT usluga.

7. Ako ključna treća strana pružatelj IKT usluga odbije prihvatiti preporuke time što zauzme drukčiji pristup od pristupa koji je savjetovalo glavno nadzorno tijelo, a takav drukčiji pristup može negativno utjecati na velik broj financijskih subjekata ili na znatan dio financijskog sektora, pri čemu pojedinačna upozorenja koja su izdala nadležna tijela nisu rezultirala dosljednim pristupima kojima se ublažava potencijalni rizika za financijsku stabilnost, glavno nadzorno tijelo može, prema potrebi i nakon savjetovanja s Nadzornim forumom, nadležnim tijelima izdati neobvezujuća mišljenja koja nisu javna radi promicanja dosljednih i konvergentnih daljnjih nadzornih mjera.

8. Nakon primitka izvješća iz članka 35. stavka 1. točke (c) nadležna tijela pri donošenju odluke iz stavka 6. ovog članka uzimaju u obzir vrstu i razmjer rizika koji ključna treća strana pružatelj IKT usluga nije uklonila te ozbiljnost neusklađenosti, vodeći računa o sljedećim kriterijima:

(a) ozbiljnosti i trajanju neusklađenosti;

(b) je li neusklađenost ukazala na ozbiljne nedostatke u postupcima, sustavima upravljanja, upravljanju rizicima i unutarnjim kontrolama ključne treće strane pružatelja IKT usluga;

(c) je li neusklađenost olakšala ili prouzročila financijska kaznena djela ili se na neki drugi način može povezati s takvim djelima;

(d) je li neusklađenost počinjena namjerno ili iz nepažnje;

(e) stvara li suspenzija ili raskid ugovornih aranžmana rizik za kontinuitet poslovanja financijskog subjekta neovisno o nastojanjima financijskog subjekta da izbjegne poremećaje u pružanju svojih usluga;

(f) ako je to primjenjivo, mišljenju zatraženom na dobrovoljnoj osnovi u skladu s člankom 5. ovog članka koje su izdala nadležna tijela imenovana ili uspostavljena u skladu s Direktivom (EU) 2022/2555 koja su odgovorna za nadzor nad ključnim ili važnim subjektom koji podliježe toj direktivi i koji je imenovan ključnom trećom stranom pružateljem IKT usluga.

Nadležna tijela financijskim subjektima omogućuju potrebno vrijeme za prilagodbu ugovornih aranžmana s ključnim trećim stranama pružateljima IKT usluga kako bi se izbjegli štetni učinci na njihovu digitalnu operativnu otpornost i kako bi im se omogućilo da uvedu izlazne strategije i tranzicijske planove iz članka 28.

9. O odluci iz stavka 6. ovog članka obavješćuju se članovi Nadzornog foruma iz članka 32. stavka 4. točaka (a), (b) i (c) i Zajednička nadzorna mreža.

Ključne treće strane pružatelji IKT usluga na koje utječu odluke iz stavka 6. u potpunosti surađuju s pogođenim financijskim subjektima, posebno u kontekstu procesa suspenzije ili raskida njihovih ugovornih aranžmana.

10. Nadležna tijela redovito informiraju glavno nadzorno tijelo o pristupima i mjerama koje su poduzela u okviru svojih nadzornih zadaća u pogledu financijskih subjekata te o ugovornim aranžmanima koje su sklopili financijski subjekti ako ključne treće strane pružatelji IKT usluga nisu djelomično ili u cijelosti prihvatili preporuke koje im je uputilo glavno nadzorno tijelo.

11. Glavno nadzorno tijelo može na zahtjev pružiti dodatna pojašnjenja o preporukama izdanima radi usmjeravanja nadležnih tijela u pogledu daljnjih mjera.

Članak 43.

Naknade za nadzor

1. Glavno nadzorno tijelo, u skladu s delegiranim aktom iz stavka 2. ovog članka, obračunava ključnim trećim stranama pružateljima IKT usluga naknade koje u potpunosti pokrivaju rashode glavnog nadzornog tijela potrebne za provedbu nadzornih zadaća na temelju ove Uredbe, uključujući povrat troškova koji mogu nastati kao rezultat rada zajedničkog tima za provjeru iz članka 40. kao i troškova savjeta koje su dali neovisni stručnjaci iz članka 32. stavka 4. drugog podstavka u vezi s pitanjima koja su obuhvaćena aktivnostima izravnog nadzora.

Iznos naknade koja se obračunava ključnoj trećoj strani pružatelju IKT usluga pokriva sve troškove koji proizlaze iz izvršavanja zadaća utvrđenih u ovom odjeljku i razmjeran je prometu te treće strane pružatelja IKT usluga.

2. Komisija je ovlaštena za donošenje delegiranog akta u skladu s člankom 57. radi dopunjavanja ove Uredbe utvrđivanjem iznosa naknada i načina njihova plaćanja do 17. srpnja 2024.

Članak 44.

Međunarodna suradnja

1. Ne dovodeći u pitanje članak 36., EBA, ESMA i EIOPA mogu, u skladu s člankom 33. uredbi (EU) br. 1093/2010, (EU) br. 1095/2010 odnosno (EU) br. 1094/2010, sklapati administrativne dogovore s regulatornim i nadzornim tijelima trećih zemalja kako bi se potaknula međunarodna suradnja u različitim financijskim sektorima u području IKT rizika povezanog s trećim stranama, osobito razvojem najboljih primjera iz prakse za preispitivanje prakse i kontrola upravljanja IKT rizicima, mjera za ublažavanje i odgovora na incidente.

2. Europska nadzorna tijela u okviru Zajedničkog odbora podnose svakih pet godina Europskom parlamentu, Vijeću i Komisiji zajedničko povjerljivo izvješće sa sažetkom nalaza relevantnih rasprava s tijelima trećih zemalja iz stavka 1., čije je težište na promjenama IKT rizika povezanog s trećim stranama i posljedicama za financijsku stabilnost, cjelovitost tržišta, zaštitu ulagatelja i funkcioniranje unutarnjeg tržišta.

POGLAVLJE VI.

Aranžmani za razmjenu informacija

Članak 45.

Aranžmani za razmjenu informacija i saznanja o kiberprijetnjama

1. Financijski subjekti mogu međusobno razmjenjivati informacije i saznanja o kiberprijetnjama, uključujući pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate, u mjeri u kojoj takva razmjena informacija i saznanja:

(a) ima za cilj poboljšanje digitalne operativne otpornosti financijskih subjekata, osobito podizanjem svijesti u vezi s kiberprijetnjama, ograničavanjem ili sprečavanjem mogućnosti širenja kiberprijetnji, potporom obrambenim sposobnostima, tehnikama otkrivanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka;

(b) odvija se u okviru pouzdanih zajednica financijskih subjekata;

(c) provodi se s pomoću aranžmana za razmjenu informacija kojima se štiti potencijalno osjetljiva priroda informacija koje se razmjenjuju i koji su uređeni pravilima poslovnog ponašanja kojima se u potpunosti poštuju poslovna tajna, zaštita osobnih podataka u skladu s Uredbom (EU) 2016/679 i smjernice o politici tržišnog natjecanja.

2. Za potrebe stavka 1. točke (c) u aranžmanima za razmjenu informacija utvrđuju se uvjeti sudjelovanja te prema potrebi pojedinosti o sudjelovanju tijela javne vlasti i svojstvu u kojem se ta tijela mogu pridružiti aranžmanima za razmjenu informacija, o sudjelovanju trećih strana pružatelja IKT usluga te o operativnim elementima, uključujući upotrebu namjenskih IT platformi.

3. Financijski subjekti obavješćuju nadležna tijela o svojem sudjelovanju u aranžmanima za razmjenu informacija iz stavka 1. nakon što se potvrdi njihovo članstvo ili, ovisno o slučaju, nakon prestanka njihova članstva, kad prestanak članstva počne proizvoditi učinke.

POGLAVLJE VII.

Nadležna tijela

Članak 46.

Nadležna tijela

Ne dovodeći u pitanje odredbe o nadzornom okviru za ključne treće strane pružatelje IKT usluga iz poglavlja V. odjeljka II. ove Uredbe, usklađenost s ovom Uredbom osiguravaju sljedeća nadležna tijela u skladu s ovlastima koje su im dodijeljene odgovarajućim pravnim aktima:

(a) za kreditne institucije i za institucije izuzete na temelju Direktive 2013/36/EU, nadležno tijelo imenovano u skladu s člankom 4. te direktive, a za kreditne institucije klasificirane kao značajne u skladu s člankom 6. stavkom 4. Uredbe (EU) br. 1024/2013, ESB u skladu s ovlastima i zadaćama koje su mu dodijeljene tom uredbom;

(b) za institucije za platni promet, uključujući institucije za platni promet izuzete na temelju Direktive (EU) 2015/2366, institucije za elektronički novac, uključujući one izuzete na temelju Direktive 2009/110/EZ, te za pružatelje usluga pružanja informacija o računu iz članka 33. stavka 1. Direktive (EU) 2015/2366, nadležno tijelo imenovano u skladu s člankom 22. Direktive (EU) 2015/2366;

(c) za investicijska društva, nadležno tijelo imenovano u skladu s člankom 4. Direktive (EU) 2019/2034 Europskog parlamenta i Vijeća ([38]);

(d) za pružatelje usluga povezanih s kriptoimovinom koji imaju odobrenje za rad na temelju Uredbe o tržištima kriptoimovine i izdavatelje tokena vezanih uz imovinu, nadležno tijelo imenovano u skladu s relevantnom odredbom te uredbe;

(e) za središnje depozitorije vrijednosnih papira, nadležno tijelo imenovano u skladu s člankom 11. Uredbe (EU) br. 909/2014;

(f) za središnje druge ugovorne strane, nadležno tijelo imenovano u skladu s člankom 22. Uredbe (EU) br. 648/2012;

(g) za mjesta trgovanja i pružatelje usluga dostave podataka, nadležno tijelo imenovano u skladu s člankom 67. Direktive 2014/65/EU i nadležno tijelo kako je definirano u članku 2. stavku 1. točki 18. Uredbe (EU) br. 600/2014;

(h) za trgovinske repozitorije, nadležno tijelo imenovano u skladu s člankom 22. Uredbe (EU) br. 648/2012;

(i) za upravitelje alternativnih investicijskih fondova, nadležno tijelo imenovano u skladu s člankom 44. Direktive 2011/61/EU;

(j) za društva za upravljanje, nadležno tijelo imenovano u skladu s člankom 97. Direktive 2009/65/EZ;

(k) za društva za osiguranje i društva za reosiguranje, nadležno tijelo imenovano u skladu s člankom 30. Direktive 2009/138/EZ;

(l) za posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju, nadležno tijelo imenovano u skladu s člankom 12. Direktive (EU) 2016/97;

(m) za institucije za strukovno mirovinsko osiguranje, nadležno tijelo imenovano u skladu s člankom 47. Direktive (EU) 2016/2341;

(n) za agencije za kreditni rejting, nadležno tijelo imenovano u skladu s člankom 21. Uredbe (EZ) br. 1060/2009;

(o) za administratore ključnih referentnih vrijednosti, nadležno tijelo imenovano u skladu s člancima 40. i 41. Uredbe (EU) 2016/1011;

([38]) Direktiva (EU) 2019/2034 Europskog parlamenta i Vijeća od 27. studenoga 2019. o bonitetnom nadzoru nad investicijskim društvima i izmjeni direktiva 2002/87/EZ, 2009/65/EZ, 2011/61/EU, 2013/36/EU, 2014/59/EU i 2014/65/EU (SL L 314, 5.12.2019., str. 64.).

(p) za pružatelje usluga skupnog financiranja, nadležno tijelo imenovano u skladu s člankom 29. Uredbe (EU) 2020/1503;

(q) za sekuritizacijske repozitorije, nadležno tijelo imenovano u skladu s člankom 10. i člankom 14. stavkom 1. Uredbe (EU) 2017/2402.

Članak 47.

Suradnja sa strukturama i tijelima osnovanima Direktivom (EU) 2022/2555

1. Da bi se potaknula suradnja i omogućile razmjene nadzornih informacija između nadležnih tijela imenovanih na temelju ove Uredbe i skupine za suradnju uspostavljene člankom 14. Direktive (EU) 2022/2555, europska nadzorna tijela i nadležna tijela mogu sudjelovati u aktivnostima skupine za suradnju kad je riječ o pitanjima koja se odnose na njihove aktivnosti nadzora nad financijskim subjektima. Europska nadzorna tijela i nadležna tijela mogu zatražiti da ih se pozove da sudjeluju u aktivnostima skupine za suradnju kad je riječ o pitanjima koja se odnose na ključne ili važne subjekte koji podliježu Direktivi (EU) 2022/2555 koji su imenovani ključnim trećim stranama pružateljima IKT usluga na temelju članka 31. ove Uredbe.

2. Prema potrebi, nadležna tijela mogu se savjetovati i dijeliti informacije s jedinstvenim kontaktnim točkama i CSIRT-ovima imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555.

3. Prema potrebi, nadležna tijela mogu zatražiti relevantne tehničke savjete i pomoć od nadležnih tijela imenovanih ili uspostavljenih u skladu Direktivom (EU) 2022/2555 i uspostaviti aranžmane za suradnju kako bi se omogućila uspostava djelotvornih i brzih koordinacijskih mehanizama.

4. Aranžmanima iz stavka 3. ovog članka mogu se, među ostalim, utvrditi postupci za koordinaciju nadzornih aktivnosti u vezi s ključnim ili važnim subjektima koji podliježu Direktivi (EU) 2022/2555 koji su imenovani ključnim trećim stranama pružateljima IKT usluga na temelju članka 31. ove Uredbe, među ostalim i za provedbu istraga i izravnog inspekcijskog nadzora u skladu s nacionalnim pravom, kao i za mehanizme za razmjenu informacija između nadležnih tijela iz ove Uredbe i nadležnih tijela imenovanih ili uspostavljenih u skladu s tom direktivom, što uključuje pristup informacijama koje zatraže potonja tijela.

Članak 48.

Suradnja tijelâ

1. Nadležna tijela blisko surađuju međusobno i, ako je to primjenjivo, s glavnim nadzornim tijelom.

2. Nadležna tijela i glavno nadzorno tijelo pravodobno razmjenjuju sve relevantne informacije o ključnim trećim stranama pružateljima IKT usluga koje su im potrebne za obavljanje njihovih zadaća na temelju ove Uredbe, posebno u pogledu utvrđenih rizika, pristupâ i mjera poduzetih u okviru nadzornih zadaća glavnog nadzornog tijela.

Članak 49.

Financijske međusektorske vježbe, komunikacija i suradnja

1. Europska nadzorna tijela, u okviru Zajedničkog odbora i u suradnji s nadležnim tijelima, sanacijskim tijelima iz članka 3. Direktive 2014/59/EU, ESB-om, Jedinstvenim sanacijskim odborom kada je riječ o informacijama koje se odnose na tijela obuhvaćena područjem primjene Uredbe (EU) br. 806/2014, ESRB-om i ENISA-om, ovisno o slučaju, mogu uspostaviti mehanizme za razmjenu djelotvornih primjera iz prakse među financijskim sektorima kako bi se na međusektorskoj razini poboljšala svijest o stanju i utvrdile zajedničke ranjivosti i rizici u pogledu kibersigurnosti.

Europska nadzorna tijela mogu osmisliti vježbe za upravljanje krizama i nepredvidive situacije, uključujući scenarije kibernapada, radi razvoja komunikacijskih kanala i postupnog omogućivanja djelotvornoga koordiniranog odgovora na razini Unije u slučaju značajnoga prekograničnog IKT incidenta ili povezane prijetnje koja ima sistemski učinak na cijeli financijski sektor Unije.

Te bi vježbe mogle biti primjerene i za testiranje ovisnosti financijskog sektora o drugim gospodarskim sektorima.

2. Nadležna tijela, europska nadzorna tijela i ESB međusobno blisko surađuju i razmjenjuju informacije radi izvršavanja svojih zadaća na temelju članaka od 47. do 54. Blisko koordiniraju svoj nadzor kako bi utvrdili i ispravili povrede ove Uredbe, razvili i promicali najbolje primjere iz prakse, olakšali suradnju, poticali dosljedno tumačenje i u slučaju neslaganja osigurali provedbu procjena koje se oslanjaju na više jurisdikcija.

Članak 50.

Administrativne kazne i korektivne mjere

1. Nadležna tijela imaju sve ovlasti nadzora, istrage i sankcioniranja potrebne za izvršavanje svojih zadaća iz ove Uredbe.

2. Ovlasti iz stavka 1. uključuju najmanje sljedeće ovlasti:

(a) pristup svim dokumentima ili podatcima u bilo kojem obliku koje nadležno tijelo smatra relevantnim za izvršavanje svojih zadaća te dobivanje ili uzimanje preslika tih dokumenata ili podataka;

(b) provedbu izravnog inspekcijskog nadzora ili istraga, koji uključuju, ali nisu ograničeni na:

   i. pozivanje predstavnika financijskih subjekata da daju usmena ili pisana objašnjenja o činjenicama ili dokumente koji se odnose na predmet i svrhu istrage te bilježenje odgovora;

   ii. obavljanje razgovora s bilo kojom fizičkom ili pravnom osobom koja pristane na razgovor u svrhu prikupljanja informacija koje se odnose na predmet istrage;

(c) zahtijevanje provedbe korektivnih mjera zbog povreda zahtjeva iz ove Uredbe.

3. Ne dovodeći u pitanje pravo država članica na izricanje kaznenih sankcija u skladu s člankom 52., države članice propisuju pravila kojima se utvrđuju odgovarajuće administrativne kazne i korektivne mjere za povrede ove Uredbe te osiguravaju njihovu djelotvornu provedbu.

Te kazne i mjere moraju biti učinkovite, proporcionalne i odvraćajuće.

4. Države članice dodjeljuju nadležnim tijelima ovlast za primjenu barem sljedećih administrativnih kazni ili korektivnih mjera za povrede ove Uredbe:

(a) izdavanje naloga fizičkoj ili pravnoj osobi da prestane s ponašanjem koje predstavlja povredu ove Uredbe i suzdrži se od ponavljanja takvog ponašanja;

(b) upućivanje zahtjeva za privremeni ili trajni prestanak postupanja ili ponašanja koje nadležno tijelo smatra protivnim odredbama ove Uredbe te sprečavanje ponavljanja takvog postupanja ili ponašanja;

(c) donošenje mjera, među ostalim i financijske prirode, kako bi se osiguralo da financijski subjekti nastave ispunjavati pravne zahtjeve;

(d) upućivanje zahtjeva, u mjeri u kojoj je to dopušteno nacionalnim pravom, za dostavu postojeće evidencije telekomunikacijskog operatera o podatkovnom prometu ako postoji opravdana sumnja u povredu ove Uredbe te ako takva evidencija može biti važna za istragu povreda ove Uredbe; i

(e) izdavanje javnih obavijesti, uključujući javne izjave u kojima se navodi identitet fizičke ili pravne osobe i priroda povrede.

5. Ako se stavak 2. točka (c) i stavak 4. primjenjuju na pravne osobe, države članice dodjeljuju nadležnim tijelima ovlast da, podložno uvjetima utvrđenima nacionalnim pravom, primijene administrativne kazne i korektivne mjere na članove upravljačkog tijela i na druge osobe koje su na temelju nacionalnog prava odgovorne za povredu.

6. Države članice osiguravaju da su sve odluke kojima se izriču administrativne kazne ili korektivne mjere iz stavka 2. točke (c) propisno obrazložene i da se protiv njih može podnijeti žalba.

Članak 51.

Izvršavanje ovlasti izricanja administrativnih kazni i korektivnih mjera

1. Nadležna tijela izvršavaju ovlasti izricanja administrativnih kazni i korektivnih mjera iz članka 50. u skladu sa svojim nacionalnim pravnim okvirima, prema potrebi i kako slijedi:

(a) izravno;

(b) u suradnji s drugim tijelima;

(c) u okviru svoje odgovornosti, delegiranjem drugim tijelima; ili

(d) podnošenjem zahtjeva nadležnim pravosudnim tijelima.

2. Pri utvrđivanju vrste i razine administrativne kazne ili korektivne mjere koja se izriče na temelju članka 50. nadležna tijela uzimaju u obzir mjeru u kojoj je povreda posljedica namjere ili nemara i sve ostale relevantne okolnosti, uključujući prema potrebi sljedeće:

(a) značajnost, težinu i trajanje povrede;

(b) stupanj odgovornosti fizičke ili pravne osobe koja je odgovorna za povredu;

(c) financijsku snagu odgovorne fizičke ili pravne osobe;

(d) veličinu ostvarene dobiti ili izbjegnutih gubitaka odgovorne fizičke ili pravne osobe, ako je to moguće utvrditi;

(e) gubitke koje su zbog povrede pretrpjele treće osobe, ako ih je moguće utvrditi;

(f) razinu suradnje odgovorne fizičke ili pravne osobe s nadležnim tijelom, ne dovodeći u pitanje potrebu da se osigura povrat dobiti koju je ta fizička ili pravna osoba ostvarila ili gubitaka koje je izbjegla;

(g) prethodne povrede koje je počinila odgovorna fizička ili pravna osoba.

Članak 52.

Kaznene sankcije

1. Države članice mogu odlučiti da neće propisati pravila o administrativnim kaznama ili korektivnim mjerama za povrede koje prema njihovu nacionalnom pravu podliježu kaznenim sankcijama.

2. Ako odluče propisati kaznene sankcije za povrede ove Uredbe, države članice moraju osigurati primjerene mjere kako bi nadležna tijela imala sve potrebne ovlasti za suradnju s pravosudnim tijelima, tijelima kaznenog progona ili kaznenopravnim tijelima u okviru svoje nadležnosti radi dobivanja specifičnih informacija povezanih s kaznenim istragama ili postupcima pokrenutima zbog povreda ove Uredbe i radi dostave tih informacija drugim nadležnim tijelima te EBA-i, ESMA-i ili EIOPA-i kako bi ispunile svoje obveze suradnje za potrebe ove Uredbe.

Članak 53.

Dužnosti obavješćivanja

Države članice obavješćuju Komisiju, ESMA-u, EBA-u i EIOPA-u o zakonima i drugim propisima kojima se provodi ovo poglavlje, uključujući sve mjerodavne kaznenopravne odredbe, do 17. siječnja 2025. Države članice bez nepotrebne odgode obavješćuju Komisiju, ESMA-u, EBA-u i EIOPA-u o svim naknadnim izmjenama tih zakona i propisa.

Članak 54.

Objava administrativnih kazni

1. Nadležna tijela bez nepotrebne odgode na svojim službenim internetskim stranicama objavljuju svaku odluku o administrativnoj kazni protiv koje se ne može podnijeti žalba, nakon što se osoba kojoj je kazna izrečena obavijesti o toj odluci.

2. Objava iz stavka 1. uključuje informacije o vrsti i prirodi povrede, identitetu odgovornih osoba te izrečenim kaznama.

3. Ako na temelju ocjene od slučaja do slučaja smatra da bi objava identiteta, u slučaju pravnih osoba, ili identiteta i osobnih podataka, u slučaju fizičkih osoba, bila nerazmjerna, što uključuje rizike u vezi sa zaštitom osobnih podataka, da bi se njome ugrozila stabilnost financijskih tržišta ili provedba kaznene istrage koja je u tijeku ili da bi se njome, u mjeri u kojoj je to moguće utvrditi, dotičnoj osobi prouzročila nerazmjerna šteta, nadležno tijelo na odluku o izricanju administrativne kazne primjenjuje jedno od sljedećih rješenja:

(a) odgađa objavu odluke do prestanka postojanja svih razloga za neobjavljivanje;

(b) objavljuje odluku na anonimnoj osnovi, u skladu s nacionalnim pravom; ili

(c) ne objavljuje odluku ako smatra da opcije iz točaka (a) i (b) nisu dostatne da se osigura neugrožavanje stabilnosti financijskih tržišta ili da takva objava nije razmjerna u odnosu na blagost izrečene kazne.

4. U slučaju odluke o objavi administrativne kazne na anonimnoj osnovi u skladu sa stavkom 3. točkom (b), objava relevantnih podataka može se odgoditi.

5. Ako nadležno tijelo objavi odluku o izricanju administrativne kazne protiv koje je podnesena žalba mjerodavnim pravosudnim tijelima, nadležna tijela bez odgode na svojim službenim internetskim stranicama dodaju tu informaciju, a kasnije i sve naknadne povezane informacije o ishodu te žalbe. Objavljuje se i svaka pravosudna odluka kojom se poništava odluka o izricanju administrativne kazne.

6. Nadležna tijela osiguravaju da svaka objava iz stavaka od 1. do 4. ostane na njihovim službenim internetskim stranicama samo tijekom razdoblja koje je potrebno za provedbu ovog članka. To razdoblje ne smije biti dulje od pet godina od objave.

Članak 55.

Čuvanje poslovne tajne

1. Sve povjerljive informacije primljene, razmijenjene ili prenesene na temelju ove Uredbe podliježu obvezi čuvanja poslovne tajne utvrđenoj u stavku 2.

2. Obveza čuvanja poslovne tajne primjenjuje se na sve osobe koje rade ili su radile za nadležna tijela na temelju ove Uredbe ili na bilo koje tijelo ili poduzeće na tržištu ili fizičku ili pravnu osobu kojima su ta nadležna tijela delegirala svoje ovlasti, uključujući revizore i stručnjake koje su nadležna tijela angažirala.

3. Informacije obuhvaćene poslovnom tajnom, uključujući razmjenu informacija između nadležnih tijela iz ove Uredbe i nadležnih tijela imenovanih ili uspostavljenih u skladu s Direktivom (EU) 2022/2555, ne smiju se odavati drugoj osobi ili tijelu, osim na temelju odredaba utvrđenih pravom Unije ili nacionalnim pravom;

4. Sve informacije razmijenjene među nadležnim tijelima na temelju ove Uredbe koje se odnose na poslovanje ili operativne uvjete i druga ekonomska ili osobna pitanja smatraju se povjerljivima i podliježu zahtjevima čuvanja poslovne tajne, osim ako nadležno tijelo u trenutku dostave informacija izjavi da se takve informacije mogu objaviti ili ako je njihova objava potrebna zbog sudskog postupka.

Članak 56.

Zaštita podataka

1. Europskim nadzornim tijelima i nadležnim tijelima dopušteno je obrađivati osobne podatke samo ako je to potrebno za izvršavanje njihovih obveza i zadaća na temelju ove Uredbe, posebno za istragu, inspekcijski nadzor, zahtjev za informacije, komunikaciju, objavu, evaluaciju, provjeru, procjenu i izradu planova nadzora. Osobni podatci obrađuju se u skladu s Uredbom (EU) 2016/679 ili Uredbom (EU) 2018/1725, ovisno o tome koja je primjenjiva.

2. Osim ako je drugim sektorskim aktima predviđeno drukčije, osobni podatci iz stavka 1. čuvaju se do obavljanja primjenjivih nadzornih dužnosti, a u svakom slučaju najdulje 15 godina, osim u slučaju sudskih postupaka koji su u tijeku i zahtijevaju da se takvi podatci čuvaju dulje.

POGLAVLJE VIII.

Delegirani akti

Članak 57.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 31. stavka 6. i članka 43. stavka 2. dodjeljuje se Komisiji na razdoblje od pet godina počevši od 17. siječnja 2024. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 31. stavka 6. i članka 43. stavka 2. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u *Službenom* listu *Europske unije* ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 31. stavka 6. i članka 43. stavka 2. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od tri mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za tri mjeseca na inicijativu Europskog parlamenta ili Vijeća.

POGLAVLJE IX.

Prijelazne i završne odredbe

Odjeljak I.

Članak 58.

Klauzula o preispitivanju

1. Komisija do 17. siječnja 2028., a nakon savjetovanja s europskim nadzornim tijelima ili s ESRB-om, ovisno o slučaju, provodi preispitivanje te Europskom parlamentu i Vijeću dostavlja izvješće, prema potrebi zajedno s prijedlogom zakonodavnog akta. Preispitivanje uključuje barem sljedeće:

(a) kriterije za imenovanje ključnih trećih strana pružatelja IKT usluga u skladu s člankom 31. stavkom 2.;

(b) dobrovoljnu prirodu obavješćivanja o ozbiljnim kiberprijetnjama iz članka 19.;

(c) režim iz članka 31. stavka 12. i ovlasti glavnog nadzornog tijela iz članka 35. stavka 1. točke (d) podtočke iv. prve alineje s ciljem evaluacije djelotvornosti tih odredaba u pogledu osiguravanja djelotvornog nadzora nad ključnim trećim stranama pružateljima IKT usluga s poslovnim nastanom u trećoj zemlji i potrebe za osnivanjem društva kćeri u Uniji.

Za potrebe prvog podstavka ove točke preispitivanje uključuje analizu režima iz članka 31. stavka 12., uključujući s obzirom na pristup financijskih subjekata Unije uslugama iz trećih zemalja i dostupnost takvih usluga na tržištu Unije te se njime uzimaju u obzir daljnji razvoj na tržištima usluga obuhvaćenih ovom Uredbom, praktično iskustvo financijskih subjekata i financijskih nadzornih tijela s obzirom na primjenu tog režima i nadzor nad tim režimom te sve relevantne promjene u području regulative i nadzora na međunarodnoj razini;

(d) primjerenost uključivanja u područje primjene ove Uredbe financijskih subjekata iz članka 2. stavka 3. točke (e) koji upotrebljavaju automatizirane sustave prodaje, s obzirom na buduća tržišna kretanja u pogledu upotrebe takvih sustava;

(e) funkcioniranje i djelotvornost Zajedničke nadzorne mreže u podupiranju dosljednosti nadzora i učinkovitosti razmjene informacija unutar nadzornog okvira.

2. U kontekstu preispitivanja Direktive (EU) 2015/2366 Komisija procjenjuje potrebu za povećanjem kiberotpornosti platnih sustava i aktivnosti obrade plaćanja te primjerenost proširenja područja primjene ove Uredbe na upravitelje platnih sustava i subjekte uključene u aktivnosti obrade plaćanja. S obzirom na tu procjenu Komisija u okviru preispitivanja Direktive (EU) 2015/2366 podnosi izvješće Europskom parlamentu i Vijeću najkasnije 17. srpnja 2023.

Na temelju tog izvješća o preispitivanju i nakon savjetovanja s europskim nadzornim tijelima, ESB-om i ESRB-om Komisija može, prema potrebi i u okviru zakonodavnog prijedloga koji može donijeti na temelju članka 108. drugog stavka Direktive (EU) 2015/2366, podnijeti prijedlog kojim se osigurava da svi upravitelji platnih sustava i subjekti uključeni u aktivnosti obrade plaćanja podliježu odgovarajućem nadzoru, uzimajući u obzir postojeći nadzor koji provodi središnja banka.

3. Komisija do 17. siječnja 2026. i nakon savjetovanja s europskim nadzornim tijelima i Odborom europskih tijela za nadzor revizije, preispituje primjerenost strožih zahtjeva za ovlaštene revizore i revizorska društva u pogledu digitalne operativne otpornosti uključivanjem ovlaštenih revizora i revizorskih društava u područje primjene ove Uredbe ili izmjenama Direktive 2006/43/EZ Europskog parlamenta i Vijeća ([39]) te Europskom parlamentu i Vijeću dostavlja izvješće, prema potrebi zajedno sa zakonodavnim prijedlogom.

Odjeljak II.

Izmjene

Članak 59.

Izmjene Uredbe (EZ) br. 1060/2009

Uredba (EZ) br. 1060/2009 mijenja se kako slijedi:

1. u Prilogu I. odjeljku A točki 4. prvi podstavak zamjenjuje se sljedećim:

„Agencija za kreditni rejting mora imati dobre administrativne i računovodstvene postupke, mehanizme unutarnje kontrole, učinkovite postupke za procjenu rizika i učinkovite mehanizme kontrole i zaštite za upravljanje IKT sustavima u skladu s Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća (*).

(*) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1..).";

2. u Prilogu III. točka 12. zamjenjuje se sljedećim:

„12. Agencija za kreditni rejting krši članak 6. stavak 2. u vezi s točkom 4. odjeljka A Priloga I. ako nema dobre administrativne ili računovodstvene postupke, mehanizme unutarnje kontrole, učinkovite postupke za procjenu rizika ili učinkovite mehanizme kontrole ili zaštite za upravljanje IKT sustavima u skladu s Uredbom (EU) 2022/2554; ili ako ne provodi ili ne održava postupke odlučivanja ili organizacijsku strukturu kako se zahtijeva tom točkom.".

Članak 60.

Izmjene Uredbe (EU) br. 648/2012

Uredba (EU) br. 648/2012 mijenja se kako slijedi:

1. članak 26. mijenja se kako slijedi:

(a) stavak 3. zamjenjuje se sljedećim:

„3. Središnja druga ugovorna strana održava organizacijsku strukturu kojom se osigurava kontinuitet i uredno funkcioniranje u obavljanju njezinih usluga i aktivnosti te upravlja tom strukturom. Koristi se primjerenim i proporcionalnim sustavima, sredstvima i postupcima, uključujući IKT sustave kojima upravlja u skladu s Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća (*).

(*) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1..).";

([39]) Direktiva 2006/43/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja, kojom se mijenjaju direktive Vijeća 78/660/EEZ i 83/349/EEZ i stavlja izvan snage Direktiva Vijeća 84/253/EEZ (SL L 157, 9.6.2006., str. 87.).

(b) stavak 6. briše se;

2. članak 34. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Središnja druga ugovorna strana uspostavlja, provodi i održava primjerenu politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, koji uključuje politiku kontinuiteta poslovanja u području IKT-a i planove odgovora i oporavka u području IKT-a uspostavljene i provedene u skladu s Uredbom (EU) 2022/2554, čiji je cilj osigurati očuvanje njezinih funkcija, pravodoban oporavak poslovanja i ispunjavanje obveza središnje druge ugovorne strane.";

(b) u stavku 3. prvi podstavak zamjenjuje se sljedećim:

„3. Kako bi se osigurala dosljedna primjena ovog članka, ESMA, nakon savjetovanja s članovima ESSB-a, izrađuje nacrt regulatornih tehničkih standarda kojima se određuju minimalni sadržaj i zahtjevi vezani uz politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, isključujući politiku kontinuiteta poslovanja i planove oporavka u slučaju katastrofe u području IKT-a.";

3. u članku 56. stavku 3. prvi podstavak zamjenjuje se sljedećim:

„3. Kako bi se osigurala dosljedna primjena ovog članka, ESMA izrađuje nacrt regulatornih tehničkih standarda kojima se određuju pojedinosti zahtjeva za registraciju iz stavka 1., osim za zahtjeve povezane s upravljanjem IKT rizicima.";

4. u članku 79. stavci 1. i 2. zamjenjuju se sljedećim:

„1. Trgovinski repozitorij utvrđuje izvore operativnog rizika i svodi ih na najmanju moguću mjeru razvojem odgovarajućih sustava, kontrola i postupaka, među ostalim i IKT sustava kojima se upravlja u skladu s Uredbom (EU) 2022/2554.

2. Trgovinski repozitorij uspostavlja, provodi i održava primjerenu politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe, koji uključuje politiku kontinuiteta poslovanja i planove odgovora i oporavka u području IKT-a uspostavljene u skladu s Uredbom (EU) 2022/2554, čiji je cilj osigurati očuvanje njegovih funkcija, pravodoban oporavak poslovanja i ispunjavanje obveza trgovinskog repozitorija.";

5. u članku 80. stavak 1. briše se;

6. u Prilogu I. odjeljak II. mijenja se kako slijedi:

(a) točke (a) i (b) zamjenjuju se sljedećim:

„(a) trgovinski repozitorij povređuje članak 79. stavak 1. time što ne utvrđuje izvore operativnog rizika ili time što te rizike ne svodi na najmanju moguću mjeru razvojem odgovarajućih sustava, kontrola i postupaka, među ostalim i IKT sustava kojima se upravlja u skladu s Uredbom (EU) 2022/2554;

(b) trgovinski repozitorij povređuje članak 79. stavak 2. time što ne uspostavlja, ne provodi ili ne održava primjerenu politiku kontinuiteta poslovanja i plan oporavka u slučaju katastrofe koji su uspostavljeni u skladu s Uredbom (EU) 2022/2554, čiji je cilj osigurati očuvanje njegovih funkcija, pravodoban oporavak poslovanja i ispunjavanje obveza trgovinskog repozitorija;";

(b) točka (c) briše se.

7. Prilog III. mijenja se kako slijedi:

(a) odjeljak II. mijenja se kako slijedi:

i. točka (c) zamjenjuje se sljedećim:

„(c) središnja druga ugovorna strana druge razine rizika krši članak 26. stavak 3. ako ne održava organizacijsku strukturu ili ne upravlja organizacijskom strukturom kojom se osiguravaju kontinuitet i uredno funkcioniranje u obavljanju njezinih usluga i aktivnosti ili ako ne upotrebljava odgovarajuće i proporcionalne sustave, sredstva ili postupke, uključujući IKT sustave kojima se upravlja u skladu s Uredbom (EU) 2022/2554;";

ii. točka (f) briše se;

(b) u odjeljku III. točka (a) zamjenjuje se sljedećim:

„(a) središnja druga ugovorna strana druge razine rizika krši članak 34. stavak 1. ako ne uspostavi, ne provodi ili ne održava primjerenu politiku kontinuiteta poslovanja i plan odgovora i oporavka uspostavljene u skladu s Uredbom (EU) 2022/2554, čiji je cilj osigurati očuvanje njezinih funkcija, pravodoban oporavak poslovanja i ispunjavanje obveza središnje druge ugovorne strane, a kojima se barem omogućuje oporavak svih transakcija u trenutku poremećaja kako bi se središnjoj drugoj ugovornoj strani omogućio siguran nastavak njezina poslovanja i okončanje namire na planirani datum;".

Članak 61.

Izmjene Uredbe (EU) br. 909/2014

Članak 45. Uredbe (EU) br. 909/2014 mijenja se kako slijedi:

1. stavak 1. zamjenjuje se sljedećim:

„1. CSD utvrđuje izvore operativnog rizika, kako unutarnje tako i vanjske, te svodi njihov utjecaj na najmanju moguću mjeru, među ostalim i primjenom odgovarajućih IKT alata, procesa i politika koji su uspostavljeni i kojima se upravlja u skladu s Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća (*)te svim drugim relevantnim primjerenim alatima, kontrolama i postupcima za druge vrste operativnog rizika, uključujući za sve sustave za namiru vrijednosnih papira kojima upravlja.

_____

(*) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1..).";

2. stavak 2. briše se;

3. stavci 3. i 4. zamjenjuju se sljedećim:

„3. Za usluge koje pruža, kao i za sve sustave za namiru vrijednosnih papira kojima upravlja, CSD uspostavlja, provodi i održava primjerenu politiku kontinuiteta poslovanja i plan za oporavak u slučaju katastrofe, uključujući politiku kontinuiteta poslovanja i planove odgovora i oporavka u području IKT-a uspostavljene u skladu s Uredbom (EU) 2022/2554, kako bi osigurao očuvanje svojih usluga, pravodoban oporavak poslovanja i ispunjavanje obveza CSD-a u slučaju događaja koji predstavljaju značajan rizik za poremećaj poslovanja.

4. Planom iz stavka 3. predviđa se oporavak svih transakcija i pozicija sudionika u trenutku poremećaja kako bi se sudionicima CSD-a omogućilo da nastave poslovati sa sigurnošću i dovrše namiru na predviđeni datum, među ostalim i osiguravanjem da ključni IT sustavi mogu nastaviti s radom nakon poremećaja kako je predviđeno u članku 12. stavcima 5. i 7. Uredbe (EU) 2022/2554.";

4. stavak 6. zamjenjuje se sljedećim:

„6. CSD utvrđuje i prati rizike te upravlja rizicima koje bi ključni sudionici u sustavima za namiru vrijednosnih papira kojima upravlja, kao i pružatelji javnih i drugih usluga te drugi CSD-ovi ili tržišne infrastrukture, mogli predstavljati za njegov rad. Na zahtjev dostavlja nadležnim i relevantnim tijelima informacije o svakom takvom utvrđenom riziku. Također bez odgode obavješćuje nadležno tijelo i relevantna tijela o svim operativnim incidentima koji proizlaze iz tih rizika, a koji nisu povezani s IKT rizikom.";

5. u stavku 7. prvi podstavak zamjenjuje se sljedećim:

„7. ESMA, u bliskoj suradnji s članovima ESSB-a, izrađuje nacrt regulatornih tehničkih standarda kojima se preciznije utvrđuju operativni rizici iz stavaka od 1. do 6., osim IKT rizika, te metode testiranja i uklanjanja rizika ili njihova svođenja na najmanju moguću mjeru, uključujući politike kontinuiteta poslovanja i planove oporavka u slučaju katastrofe iz stavaka 3. i 4. i metode njihove procjene.".

Članak 62.

Izmjene Uredbe (EU) br. 600/2014

Uredba (EU) br. 600/2014 mijenja se kako slijedi:

1. članak 27.g mijenja se kako slijedi:

   (a) stavak 4. zamjenjuje se sljedećim:

   „4. APA ispunjava zahtjeve u pogledu sigurnosti mrežnih i informacijskih sustava utvrđene u Uredbi (EU) 2022/2554 Europskog parlamenta i Vijeća (*).

   _____

   (*) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1..).";

   (b) u stavku 8. točka (c) zamjenjuje se sljedećim:

   „(c) konkretni organizacijski zahtjevi utvrđeni u stavcima 3. i 5.";

2. članak 27.h mijenja se kako slijedi:

   (a) stavak 5. zamjenjuje se sljedećim:

   „5. CTP ispunjava zahtjeve u pogledu sigurnosti mrežnih i informacijskih sustava utvrđene u Uredbi (EU) 2022/2554.";

   (b) u stavku 8. točka (e) zamjenjuje se sljedećim:

   „(e) konkretne organizacijske zahtjeve utvrđene u stavku 4.";

3. članak 27.i mijenja se kako slijedi:

   (a) stavak 3. zamjenjuje se sljedećim:

   „3. Ovlašteni mehanizam izvješćivanja ispunjava zahtjeve u pogledu sigurnosti mrežnih i informacijskih sustava utvrđene u Uredbi (EU) 2022/2554.";

   (b) u stavku 5. točka (b) zamjenjuje se sljedećim:

   „(b) konkretni organizacijski zahtjevi utvrđeni u stavcima 2. i 4.".

Članak 63.

Izmjena Uredbe (EU) br. 2016/1011

U članku 6. Uredbe (EU) 2016/1011 dodaje se sljedeći stavak:

„6. Kad je riječ o ključnim referentnim vrijednostima, administrator ima uspostavljene dobre administrativne i računovodstvene postupke, mehanizme unutarnje kontrole, djelotvorne postupke za procjenu rizika i djelotvorne mehanizme kontrole i osiguranja za upravljanje IKT sustavima u skladu s Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća (*).

_____

(*) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1..).".

Članak 64.

Stupanje na snagu i primjena

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od 17. siječnja 2025.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Strasbourgu 14. prosinca 2022.

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*
R. METSOLA	M. BEK