



Crna Gora
Vlada Crne Gore

CRNA GORA SKUPŠTINA CRNE GORE	
PRIMLJENO: 16. 01.	20 26. GOD.
KLASIFIKACIONI BROJ: 10-1/26-1	
VEZA:	
EPA: 848xxym	
SKRAĆENICA:	PRILOG:

Br: 11-011/26-30/5

15. januar 2026. godine

SKUPŠTINA CRNE GORE

Gospodin Andrija Mandić, predsjednik

Vlada Crne Gore, na sjednici od 14. januara 2026. godine, utvrdila je **PREDLOG ZAKONA O DIGITALNOJ OPERATIVNOJ OTPORNOSTI FINANSIJSKOG SEKTORA***, koji Vam u prilogu dostavljamo radi stavljanja u proceduru Skupštine Crne Gore.

Vlada predlaže Skupštini da, u skladu sa članom 151 Poslovnika Skupštine Crne Gore („Službeni list RCG“, br. 51/06 i 66/06 i „Službeni list CG“ br. 88/09, 80/10, 39/11, 25/12, 49/13, 32/14, 42/15, 52/17, 17/18, 47/19, 112/20, 129/20, 65/21, 48/24 i 80/24), ovaj zakon donese po hitnom postupku iz razloga koji su sadržani u Obrazloženju Predloga zakona.

Za predstavnike Vlade, koji će učestvovati u radu Skupštine i njenih radnih tijela prilikom razmatranja Predloga ovog zakona, određeni su NOVICA VUKOVIĆ, ministar finansija i mr ALEKSANDRA POPOVIĆ, generalna direktorica Direktorata za finansijski sistem i koordinaciju politika u Ministarstvu finansija.

Vlada preporučuje Skupštini Crne Gore da, prilikom razmatranja Predloga ovog zakona, pozove dr Irenu Radović, guvernerku Centralne banke Crne Gore, da učestvuje u radu Skupštine i njenih radnih tijela.

PREDSJEDNIK
mr Milojko Spajić, s. r.

**ZAKON
O DIGITALNOJ OPERATIVNOJ OTPORNOSTI FINANSIJSKOG SEKTORA***

I. OSNOVNE ODREDBE

Predmet

Član 1

Ovim zakonom utvrđuju se zahtjevi, postupci i mjere za obezbjeđivanje visokog nivoa digitalne operativne otpornosti finansijskog sektora, uključujući zahtjeve za bezbjednost mrežnih i informacionih sistema koji podržavaju poslovanje finansijskih subjekata, kao i druga pitanja od značaja za digitalnu operativnu otpornost finansijskog sektora.

Primjena

Član 2

(1) Ovaj zakon primjenjuje se na subjekte finansijskog sektora (u daljem tekstu: finansijski subjekt), i to:

- 1) kreditnu instituciju;
- 2) platnu instituciju sa sjedištem u Crnoj Gori;
- 3) registrovanog pružaoca usluge informacija o računu sa sjedištem u Crnoj Gori;
- 4) instituciju za elektronski novac sa sjedištem u Crnoj Gori;
- 5) investiciono društvo;
- 6) centralno klirinško depozitarno društvo;
- 7) centralnu drugu ugovornu stranu;
- 8) mjesto trgovanja;
- 9) trgovinski repozitorij;
- 10) društvo za upravljanje alternativnim investicionim fondom;
- 11) društva za upravljanje otvorenim investicionim fondom sa javnom ponudom;
- 12) instituciju za profesionalnu penzionu štednju;
- 13) pružaoca usluga dostave podataka;
- 14) administratora ključnih referentnih vrijednosti;
- 15) društvo za osiguranje;
- 16) društvo za reosiguranje;
- 17) podružnicu stranog društava za osiguranje;
- 18) podružnicu stranog društava za reosiguranje;
- 19) društvo za posredovanje u osiguranju;
- 20) sporednog posrednika u osiguranju;
- 21) preduzetnika posrednika u osiguranju;
- 22) društvo za zastupanje u osiguranju;
- 23) sporednog zastupnika u osiguranju;
- 24) preduzetnika zastupnika u osiguranju;
- 25) agenciju za pružanje drugih usluga u osiguranju;
- 26) pružaoca usluga povezanih sa kriptovimovinom;
- 27) izdavaoca tokena vezanih za imovinu.

(2) Ovaj zakon ne primjenjuje se na:

- 1) Razvojnu banku Crne Gore;

- 2) društva za osiguranje i društva za reosiguranje iz člana 3 i 4 Zakona o osiguranju ("Službeni list CG", broj 33/25);
- 3) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju koji su klasifikovani kao mikro, mali ili srednji finansijski subjekti;
- 4) institucije za profesionalnu penzionu štednju koje upravljaju penzionim šemama sa ukupno najviše 15 članova, a koje su uređene zakonom kojim se uređuju dobrovoljni penzioni fondovi.

(3) Ovaj zakon ne utiče na odredbe zakona kojim se uređuju nadležnosti državnih organa u vezi sa zaštitom javne bezbjednosti, nacionalne bezbjednosti i odbrane.

Nadležni organ

Član 3

(1) Nadležni organ, u smislu ovog zakona, je organ koji je u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta iz člana 2 stav 1 ovog zakona nadležan za kontrolu, superviziju, odnosno nadzor tog subjekta, i to:

- 1) za finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona, Centralna banka Crne Gore (u daljem tekstu: Centralna banka);
- 2) za finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona, Komisija za tržište kapitala Crne Gore (u daljem tekstu: Komisija);
- 3) za finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona, Agencija za nadzor osiguranja (u daljem tekstu: Agencija);
- 4) za finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona, organ utvrđen posebnim zakonom.

(2) Nadležni organi iz stava 1 ovog člana dužni su da međusobno sarađuju i razmjenjuju informacije i podatke potrebne za sprovođenje ovog zakona.

(3) Protiv rješenja nadležnog organa koje se donosi u skladu sa odredbama ovog zakona može se tužbom pokrenuti upravni spor.

(4) U upravnom sporu protiv rješenja nadležnog organa iz stava 3 ovog člana, nadležni sud ne može meritorno odlučivati o predmetu upravnog spora za čije rješavanje je ovim zakonom utvrđena nadležnost nadležnog organa.

Digitalna operativna otpornost

Član 4

Digitalna operativna otpornost, u smislu ovog zakona, je sposobnost finansijskog subjekta da izgradi, obezbijedi i preispituje svoj operativni integritet i pouzdanost, na način da, direktno ili indirektno kroz korišćenje usluga koje pružaju treće strane, odnosno pružaoci usluga informaciono komunikacionih tehnologija (u daljem tekstu: IKT), stvara uslove za primjenu svih IKT kapaciteta neophodnih za bezbjednost mrežnih i informacionih sistema koje koristi i koji podržavaju kontinuirano pružanje finansijskih usluga tog subjekta i očuvanje njihovog kvaliteta, uključujući i u slučaju poremećaja.

Princip proporcionalnosti

Član 5

(1) Finansijski subjekt je dužan da primjenjuje odredbe ovog zakona srazmjerno svojoj veličini, ukupnom rizičnom profilu, prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, na način utvrđen ovim zakonom.

(2) Nadležni organ razmatra primjenu principa proporcionalnosti iz stava 1 ovog člana prilikom procjene konzistentnosti sistema finansijskog subjekta za upravljanje IKT rizicima, uzimajući u obzir izvještaje koji se dostavljaju na zahtjev nadležnog organa u skladu sa članom 11 stav 3 ovog zakona, odnosno članom 21 ovog zakona.

Klasifikacija finansijskih subjekata prema veličini

Član 6

(1) U smislu ovog zakona, u zavisnosti od prosječnog broja zaposlenih, ukupnog prihoda na godišnjem nivou i ukupne aktive, finansijski subjekti se klasifikuju kao:

1) mikro finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini manji od deset; i
- ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu do 2.000.000,00 eura;

2) mali finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini u rasponu od deset do 49; i
- ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu u rasponu od 2.000.000,01 eura do 10.000.000,00 eura;

3) srednji finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini manji od 250; i
- ostvaruju ukupan prihod na godišnjem nivou do 50.000.000,00 eura i/ili ukupnu aktivu do 43.000.000,00 eura;

4) ostali finansijski subjekti, koji se ne mogu klasifikovati kao mikro, mali ili srednji finansijski subjekti, u skladu sa tač. 1 do 3 ovog stava.

(2) Klasifikaciju u skladu sa kriterijumima iz stava 1 ovog člana, vrši finansijski subjekt na dan sastavljanja finansijskih iskaza i podatke na osnovu kojih je izvršena klasifikacija koristi za narednu poslovnu godinu.

(3) Izuzetno od stava 2 ovog člana, novoosnovani finansijski subjekt klasifikuje se na osnovu podataka iz finansijskih iskaza tekuće poslovne godine i broja mjeseci poslovanja, a utvrđeni podaci koriste se za tekuću i narednu poslovnu godinu.

(4) Prosječan broj zaposlenih iz stava 1 ovog člana, izračunava se na način da se ukupan broj zaposlenih krajem svakog mjeseca, uključujući i zaposlene u inostranstvu, podijeli sa brojem mjeseci u poslovnoj godini, odnosno brojem mjeseci poslovanja finansijskog subjekta.

(5) Ako na dan sastavljanja bilansa stanja, u dvije uzastopne finansijske godine dođe do odstupanja od graničnih vrijednosti iz stava 1 ovog člana, finansijski subjekt dužan je da izvrši klasifikaciju u odgovarajuću kategoriju za narednu poslovnu godinu.

(6) Izuzetno od stava 1 tačka 1 ovog člana, finansijski subjekt koji je mjesto trgovanja, centralna druga ugovorna strana, trgovinski repozitorij ili centralno klirinško deponitarno društvo i ispunjava uslove da bude klasifikovan kao mikro finansijski subjekt, klasifikuje se kao ostali finansijski subjekt.

Upotreba rodno osjetljivog jezika

Član 7

Izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

Značenje izraza

Član 8

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) **mrežni i informacijski sistem** je:

- elektronska komunikacijska mreža, odnosno sistem prenosa koji se zasniva na stalnoj infrastrukturi ili centralizovanom upravljačkom kapacitetu i obuhvata, gdje je primjenljivo, uređaje za komutaciju ili usmjeravanje i druga sredstva, uključujući pasivne mrežne elemente, koji omogućavaju prenos signala pomoću žičanih, radio, optičkih ili drugih elektromagnetnih sistema, uključujući satelitske mreže, fiksne (sa komutacijom kola i paketa, uključujući internet) i mobilne mreže, elektroenergetske kablovske sisteme, u dijelu koji se koristi za prenos signala, mreže koje se koriste za prenos i distribuciju radijskih i televizijskih programa bez obzira na vrstu informacije koja se prenosi;
- svaki uređaj ili skup povezanih ili međuzavisnih uređaja, od kojih najmanje jedan programski izvršava automatsku obradu podataka u elektronskom obliku; ili
- podaci u elektronskom obliku koji se čuvaju, obrađuju, dobijaju ili prenose na način iz al. 1 i 2 ove tačke, u svrhu rada, korišćenja, zaštite i održavanja tih mrežnih i informacijskih sistema;

2) **zastarjeli IKT sistem** je IKT sistem koji je dostigao kraj svog životnog ciklusa, a koji zbog tehnoloških ili komercijalnih razloga nije pogodan za nadogradnje ili popravke ili za koji njegov dobavljač ili treća strana koja pruža IKT usluge prestane da pruža podršku, ali je i dalje u upotrebi i podržava funkcije finansijskog subjekta;

3) **bezbjednost mrežnih i informacijskih sistema** je sposobnost mrežnih i informacijskih sistema da se, na određenom nivou pouzdanosti, odupru svakom događaju koji može da ugrozi dostupnost, autentičnost, integritet ili povjerljivost podataka koji se čuvaju, prenose ili obrađuju, kao i usluga koje ti sistemi nude ili kojima se preko njih pristupa;

4) **IKT rizik** je svaka razumno prepoznatljiva okolnost koja se odnosi na korišćenje mrežnih i informacijskih sistema, a koja, ukoliko nastane, može da dovede do negativnih uticaja u digitalnom ili fizičkom okruženju i ugrozi bezbjednost mrežnih i informacijskih sistema, bilo kog tehnološki zavisnog alata ili procesa, poslovnih operacija i procesa ili pružanja usluga;

5) **informaciona imovina** je skup materijalnih ili nematerijalnih informacija, koje je potrebno zaštititi;

6) **IKT imovina** je softverska ili hardverska imovina u mrežnim i informacijskim sistemima koje koristi finansijski subjekt;

7) **IKT incident** je jedan ili više povezanih događaja koje finansijski subjekt nije planirao, a koji narušavaju bezbjednost mrežnih i informacijskih sistema i negativno utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka, ili na usluge koje finansijski subjekt pruža;

8) **operativni ili sigurnosni incident povezan sa plaćanjem** je jedan ili više povezanih događaja, bez obzira da li su povezani sa IKT-om, koje finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona nije planirao, a koji negativno

- utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka povezanih sa plaćanjem, ili na usluge povezane sa plaćanjem koje finansijski subjekt pruža;
- 9) **značajan IKT incident** je IKT incident koji ima visok nivo negativnog uticaja na mrežne i informacione sisteme koji podržavaju kritične ili važne funkcije finansijskog subjekta;
- 10) **značajan operativni ili sigurnosni incident** povezan sa plaćanjem je operativni ili sigurnosni incident povezan sa plaćanjem koji ima visok nivo negativnog uticaja na usluge povezane sa plaćanjem koje se pružaju;
- 11) **sajber prijetnja** je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na mrežne i informacione sisteme, korisnike tih sistema i druga lica;
- 12) **ozbiljna sajber prijetnja** je sajber prijetnja čije tehničke karakteristike ukazuju na to da bi mogla dovesti do značajnog IKT incidenta ili značajnog operativnog ili sigurnosnog incidenta povezanog sa plaćanjem;
- 13) **sajber napad** je zlonamjerni IKT incident izazvan pokušajem bilo kojeg aktera da uništi, razotkrije, izmijeni, onemogući, ukrade imovinu, stekne neovlašćeni pristup imovini ili je neovlašćeno koristi;
- 14) **saznanja o prijetnjama** su informacije koje su agregirane, prilagođene, analizirane, protumačene ili dopunjene radi utvrđivanja potrebe donošenja odluka i omogućavanja adekvatnog i dovoljnog razumijevanja u cilju ublažavanja posljedica IKT incidenta ili sajber prijetnje, uključujući informacije o tehničkim detaljima sajber napada, licima odgovornim za napad, njihovom načinu djelovanja i motivima;
- 15) **ranjivost** je slabost, podložnost ili nedostatak resursa, sistema, procesa ili kontrole koju sajber prijetnja može iskoristiti;
- 16) **penetraciono testiranje vođeno prijetnjama (TLPT)** je kontrolisano, prilagođeno testiranje kritičnih produkcionih sistema koje finansijski subjekt koristi, zasnovano na saznanjima o prijetnjama, odnosno testiranje crvenog tima, koje se sprovodi u skladu sa okvirom koji oponaša taktike, tehnike i postupke stvarnih zlonamjernih aktera za koje se vjeruje da predstavljaju realnu sajber prijetnju;
- 17) **TLPT organ druge države članice** je:
- jedinstveni javni organ u finansijskom sektoru sa sjedištem u drugoj državi članici, koji je imenovan u skladu sa članom 26 stav 9 Regulative (EU) br. 2022/2554;
 - nadležni organ sa sjedištem u drugoj državi članici kojem je povjereno izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, u skladu sa članom 26 stav 10 Regulative (EU) br. 2022/2554;
 - nadležni organ iz člana 46 Regulative (EU) br. 2022/2554, sa sjedištem u drugoj državi članici.
- 18) **zajednički TLPT** je TLPT, koji nije objedinjeni TLPT iz člana 30 stav 2 ovog zakona, a kojim je obuhvaćeno više finansijskih subjekata koji koriste IKT usluge koje pruža grupni pružalac IKT usluga ili pripadaju istoj grupi i zajednički koriste IKT sisteme;
- 19) **IKT rizik povezan sa trećim stranama** je IKT rizik kojem finansijski subjekt može biti izložen zbog korišćenja IKT usluga koje pružaju treće strane ili njihovi podizvođači, uključujući i na osnovu ugovora o eksteralizaciji;

- 20) **treća strana koja pruža IKT usluge** je pravno ili fizičko lice koje pruža IKT usluge;
- 21) **grupni pružalac IKT usluga** je pravno lice koje je dio finansijske grupe i koje pruža IKT usluge pretežno finansijskim subjektima koji su dio iste grupe ili finansijskim subjektima koji pripadaju istom institucionalnom sistemu zaštite, uključujući i njihova matična pravna lica, zavisna pravna lica, filijale i druge subjekte koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom;
- 22) **IKT usluge** su digitalne usluge i usluge vezane za podatke koje se pomoću IKT sistema, kontinuirano pružaju jednom ili više internih ili eksternih korisnika, uključujući usluge iznajmljivanja IKT opreme („hardver kao usluga“) i hardverske usluge koje uključuju pružanje tehničke podrške od strane pružaoca hardvera putem ažuriranja softvera ili firmvera, osim tradicionalnih analognih telefonskih usluga;
- 23) **kritična ili važna funkcija** je funkcija čiji bi poremećaj značajno narušio finansijske rezultate finansijskog subjekta, pouzdanost, kontinuitet njegovih usluga i aktivnosti, ili funkcija čiji bi prekidi, neispravno ili neuspješno izvršavanje značajno narušili sposobnost tog subjekta da kontinuirano ispunjava uslove i obaveze utvrđene dozvolom za rad ili druge obaveze u skladu sa propisima kojima se uređuje pružanje finansijskih usluga;
- 24) **kritična treća strana koja pruža IKT usluge** je treća strana koja pruža IKT usluge i koja je određena kao kritična u skladu sa članom 31 Regulative (EU) br. 2022/2554;
- 25) **treća strana koja pruža IKT usluge sa sjedištem u trećoj zemlji** je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa finansijskim subjektom za pružanje IKT usluga;
- 26) **treća zemlja** je strana država koja nije država članica i država članica do pristupanja Crne Gore Evropskoj uniji;
- 27) **država članica** je država članica Evropske unije i država potpisnica Ugovora o Evropskom ekonomskom prostoru;
- 28) **zavisno pravno lice** je pravno lice koje je pod kontrolom matičnog pravnog lica, uključujući i bilo koje pravno lice koje je pod kontrolom krajnjeg matičnog pravnog lica;
- 29) **grupa** je matično pravno lice i sva njegova zavisna pravna lica;
- 30) **matično pravno lice** ima značenje utvrđeno zakonom kojim se uređuje računovodstvo;
- 31) **IKT podizvođač sa sjedištem u trećoj zemlji** je IKT podizvođač koji je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa trećom stranom koja pruža IKT usluge, bez obzira na sjedište treće strane koja pruža IKT usluge;
- 32) **rizik IKT koncentracije** je izloženost prema jednoj ili više povezanih trećih strana koje pružaju IKT usluge, kojom se stvara zavisnost od tih trećih strana na način da njihova nedostupnost, propast ili druga vrsta nedostatka može potencijalno da ugrozi sposobnost finansijskog subjekta da obavlja kritične ili važne funkcije, ili prouzrokuje druge vrste negativnih uticaja, uključujući značajne gubitke, ili ugrozi finansijsku stabilnost tržišta kao cjeline;
- 33) **organ upravljanja** je:
- jedan ili više organa finansijskog subjekta, koji su u skladu sa propisima ovlašćeni da utvrđuju strategiju, ciljeve i opšte usmjerenje tog finansijskog

subjekta i koji vrše nadzor i prate odlučivanje u vezi sa upravljanjem i uključuje lica koja stvarno upravljaju poslovanjem tog finansijskog subjekta; ili

- lica koja imaju ovlaštenja jednaka ovlaštenjima iz alineje 1 ove tačke i koja, u skladu sa propisima, vode poslove finansijskog subjekta ili imaju ključne funkcije;

- 34) **kreditna institucija** ima značenje utvrđeno zakonom kojim se uređuje poslovanje kreditnih institucija;
- 35) **platna institucija sa sjedištem u Crnoj Gori** ima značenje utvrđeno zakonom kojim se uređuje platni promet;
- 36) **registrovani pružalac usluge informacija o računu sa sjedištem u Crnoj Gori** ima značenje utvrđeno zakonom kojim se uređuje platni promet;
- 37) **institucija za elektronski novac sa sjedištem u Crnoj Gori** ima značenje utvrđeno zakonom kojim se uređuje platni promet;
- 38) **investiciono društvo** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 39) **malo i nepovezano investiciono društvo** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 40) **centralno klirinško depozitarno društvo** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 41) **centralna druga ugovorna strana** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 42) **mjesto trgovanja** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 43) **trgovinski repozitorij** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 44) **društvo za upravljanje alternativnim investicionim fondom** ima značenje utvrđeno zakonom kojim se uređuje poslovanje alternativnih fondova;
- 45) **društvo za upravljanje otvorenim investicionim fondom** sa javnom ponudom ima značenje utvrđeno zakonom kojim se uređuje poslovanje otvorenih investicionih fondova sa javnom ponudom;
- 46) **institucija za profesionalnu penzionu štednju** ima značenje utvrđeno zakonom koji uređuje dobrovoljne penzione fondove;
- 47) **mala institucija za profesionalnu penzionu štednju** je institucija za profesionalnu penzionu štednju koja upravlja penzionim programima koji ukupno imaju manje od 100 članova;
- 48) **pružalac usluga dostave podataka** ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;
- 49) **administrator ključnih referentnih vrijednosti** ima značenje utvrđeno zakonom kojim se uređuju referentne vrijednosti;
- 50) **društvo za osiguranje** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 51) **društvo za reosiguranje** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 52) **podružnica stranog društava za osiguranje** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

- 53) **podružnica stranog društava za reosiguranje** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 54) **društvo za posredovanje u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 55) **sporedni posrednik u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 56) **preduzetnik posrednik u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 57) **društvo za zastupanje u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 58) **sporedni zastupnik u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 59) **preduzetnik zastupnik u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 60) **agencija za pružanje drugih usluga u osiguranju** ima značenje utvrđeno zakonom kojim se uređuje osiguranje;
- 61) **pružalac usluga povezanih sa kriptovimovinom** ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;
- 62) **izdavalac tokena vezanih za imovinu** ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;
- 63) **javni organ** je svaki organ državne uprave, drugi državni organ ili organ sa javnim ovlašćenjima, uključujući Centralnu banku Crne Gore;
- 64) **ECB** je Evropska centralna banka;
- 65) **EBA** je Evropski bankarski regulator;
- 66) **EIOPA** je Evropski nadzorni organ za osiguranje i profesionalno penzijsko osiguranje;
- 67) **ESCB** je Evropski sistem centralnih banaka;
- 68) **ESMA** je Evropski nadzorni organ za hartije od vrijednosti i tržište kapitala.

II. UPRAVLJANJE IKT RIZICIMA

Korporativno upravljanje i organizacija

Član 9

(1) Organ upravljanja finansijskog subjekta dužan je da obezbijedi da finansijski subjekt postupa u skladu sa odredbama ovog zakona.

(2) Finansijski subjekt dužan je da uspostavi sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima, u skladu sa članom 10 st. 5 i 6 ovog zakona, radi postizanja visokog nivoa digitalne operativne otpornosti.

(3) Organ upravljanja finansijskog subjekta dužan je da utvrdi, odobri i nadzire sva pravila, postupke, procese, mehanizme, mjere i resurse povezane sa sistemom upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona i da obezbijedi njihovu primjenu, i u tom cilju naročito da:

- 1) uspostavlja politike sa ciljem održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka;

- 2) jasno utvrđuje ovlašćenja, zaduženja i odgovornosti za obavljanje svih poslova povezanih sa IKT i uspostavlja odgovarajuće mehanizme upravljanja kako bi se, na svim organizacionim nivoima, obezbijedila efikasna i blagovremena komunikacija, saradnja i koordinacija u vezi sa obavljanjem tih poslova;
 - 3) utvrđuje strategiju digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona, uključujući i odgovarajući nivo tolerancije finansijskog subjekta prema IKT riziku iz člana 12 stav 2 tačka 2 ovog zakona;
 - 4) usvaja i periodično preispituje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona i planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i nadzire njihovu primjenu;
 - 5) odobrava i periodično preispituje planove interne revizije u IKT oblasti, njihove značajne izmjene i da redovno razmatra rezultate revizija u IKT oblasti;
 - 6) donosi i periodično preispituje odgovarajući plan raspodjele finansijskih sredstava za ispunjavanje svih potreba finansijskog subjekta u pogledu digitalne operativne otpornosti, uključujući i sprovođenje relevantnih programa za podizanje svijesti o IKT bezbjednosti i obuka o digitalnoj operativnoj otpornosti iz člana 19 stav 10 ovog zakona i sticanje znanja i vještina u IKT oblasti za sve zaposlene;
 - 7) usvaja i periodično preispituje politiku o korišćenju IKT usluga koje pružaju treće strane koje pružaju IKT usluge;
 - 8) na nivou cijele organizacije uspostavlja mehanizme izvještavanja za blagovremeno i adekvatno informisanje u vezi sa:
 - zaključenim ugovorima sa trećim stranama koje pružaju IKT usluge;
 - svim planiranim značajnim promjenama u vezi sa trećim stranama koje pružaju IKT usluge;
 - potencijalnim uticajem promjena iz alineje 2 ove tačke na kritične ili važne funkcije, uključujući rezime analize rizika za procjenu uticaja tih promjena;
 - IKT incidentima, a najmanje o značajnim IKT incidentima i njihovom uticaju, kao i o odgovoru, oporavku i korektivnim mjerama.
- (4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi organizacioni dio odgovoran za praćenje realizacije ugovora zaključenih sa trećim stranama koje pružaju IKT usluge, ili da imenuje člana višeg rukovodstva koji će biti odgovoran za nadzor izloženosti prema povezanom riziku i pripadajuće dokumentacije.
- (5) Članovi organa upravljanja dužni su da aktivno unapređuju znanje i vještine potrebne za razumijevanje i procjenu IKT rizika i njegovog uticaja na poslovanje finansijskog subjekta, uključujući i kroz redovne posebne obuke, srazmjerno prirodi rizika kojim se upravlja.

Sistem upravljanja IKT rizicima

Član 10

(1) Finansijski subjekt je dužan da uspostavi pouzdan, sveobuhvatan i dobro dokumentovan sistem upravljanja IKT rizicima, kao dio opšteg sistema upravljanja rizicima, kojim se omogućava brzo, efikasno i sveobuhvatno tretiranje IKT rizika i obezbjeđuje visok nivo digitalne operativne otpornosti.

(2) Sistem upravljanja IKT rizicima iz stava 1 ovog člana, najmanje obuhvata strategije, politike, procedure, IKT protokole i alate potrebne za pravilnu i adekvatnu

zaštitu cjelokupne informacione imovine i IKT imovine, uključujući softver, servere i ostali hardver i zaštitu svih relevantnih fizičkih komponenti i infrastrukture, kao što su prostorije, računarski centri i posebna osjetljiva područja, kako bi se obezbijedilo da je sva informaciona imovina i IKT imovina adekvatno zaštićena od rizika, uključujući oštećenja, neovlašćen pristup ili korišćenje.

(3) Finansijski subjekt je dužan da, u skladu sa sistemom upravljanja IKT rizicima, svede na najmanju moguću mjeru uticaj IKT rizika, primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata iz stava 2 ovog člana.

(4) Finansijski subjekt je dužan da nadležnom organu, na njegov zahtjev, dostavi potpune i ažurne informacije o IKT rizicima i sistemu upravljanja IKT rizicima iz stava 1 ovog člana.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odgovornost za upravljanje i nadzor nad IKT rizikom dodijeli kontrolnoj funkciji i da obezbijedi odgovarajući nivo njene nezavisnosti, na način da se izbjegava sukob interesa.

(6) Finansijski subjekt je dužan da obezbijedi međusobnu nezavisnost i razdvajanje poslova u kojima IKT rizik nastaje, poslova kontrolnih funkcija i poslova interne revizije, u skladu sa modelom tri linije odbrane ili internim modelom za upravljanje i kontrolu rizika.

Unaprjeđivanje i revizija sistema upravljanja IKT rizicima

Član 11

(1) Finansijski subjekt je dužan da kontinuirano unaprjeđuje sistem upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona na osnovu iskustava stečenih kroz njegovu praktičnu primjenu i praćenje, kao i da taj sistem preispituje i ažurira:

- 1) najmanje jednom godišnje;
- 2) u slučaju značajnog IKT incidenta;
- 3) na zahtjev nadležnog organa;
- 4) u skladu sa rezultatima testiranja digitalne operativne otpornosti;
- 5) u skladu sa zaključcima revizije.

(2) Izuzetno od stava 1 tačka 1 ovog člana, finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da preispituje i ažurira sistem upravljanja IKT rizicima iz stava 1 ovog člana periodično.

(3) Finansijski subjekt je dužan da izvještaj o preispitivanju i ažuriranju iz st. 1 i 2 ovog člana dostavi nadležnom organu, na njegov zahtjev.

(4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi redovne interne revizije sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, u skladu sa planom revizije, od strane nezavisnih revizora koji posjeduju znanje, vještine i iskustvo u oblasti IKT rizika.

(5) Učestalost i predmet revizija iz stava 4 ovog člana moraju biti srazmjerni IKT riziku finansijskog subjekta.

(6) Finansijski subjekt je dužan da uspostavi formalan proces koji omogućava blagovremeno otklanjanje ključnih nepravilnosti i nedostataka utvrđenih revizijom iz stava 4 ovog člana, kao i adekvatnu provjeru i praćenje tog postupka.

Strategija digitalne operativne otpornosti

Član 12

(1) Finansijski subjekt je dužan da u strategiji digitalne operativne otpornosti, koja predstavlja sastavni dio sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, utvrdi način primjene tog sistema.

(2) Strategija iz stava 1 ovog člana mora da obuhvati opšte kriterijume i metode za tretiranje IKT rizika i postizanje konkretnih IKT ciljeva, a najmanje mora da:

- 1) opisuje i objašnjava kako sistem za upravljanje IKT rizicima podržava poslovnu strategiju i ciljeve finansijskog subjekta;
- 2) utvrđuje nivo tolerancije prema IKT riziku, u skladu sa sklonošću finansijskog subjekta ka preuzimanju rizika, i sadrži analizu prihvatljivog uticaja IKT poremećaja;
- 3) definiše jasne ciljeve u oblasti informacione bezbjednosti, uključujući ključne indikatore uspješnosti i ključne metrike rizika;
- 4) opisuje i objašnjava referentnu, odnosno ciljanu IKT arhitekturu i sve promjene potrebne za postizanje konkretnih poslovnih ciljeva;
- 5) okvirno navodi različite mehanizme uspostavljene radi otkrivanja IKT incidenata, sprečavanja njihovog uticaja i obezbjeđivanja zaštite od tog uticaja;
- 6) jasno prikazuje postojeće stanje digitalne operativne otpornosti, na osnovu informacija o broju prijavljenih značajnih IKT incidenata i efikasnosti preventivnih mjera;
- 7) predviđa sprovođenje testiranja digitalne operativne otpornosti, u skladu sa odredbama čl. 27 do 32 ovog zakona;
- 8) utvrđuje strategiju komunikacije u slučaju IKT incidenata o kojima se informacije saopštavaju u skladu sa članom 20 ovog zakona.

(3) Finansijski subjekt može, da utvrdi sveobuhvatnu strategiju IKT nabavke od više dobavljača, na nivou grupe ili subjekta, kojom se identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge i obrazlažu razlozi za diverzifikaciju dobavljača.

(4) Finansijski subjekt može, u skladu sa zakonom, da povjeri obavljanje poslova provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima subjektima unutar grupe ili drugim subjektima.

(5) U slučaju iz stava 4 ovog člana, finansijski subjekt zadržava odgovornost za usklađenost sa zahtjevima za upravljanje IKT rizicima, kao i za provjeru te usklađenosti.

IKT sistemi, protokoli i alati

Član 13

Finansijski subjekt je dužan da, radi tretiranja i upravljanja IKT rizikom, koristi i održava ažurnim IKT sisteme, protokole i alate koji moraju biti:

- 1) primjereni za obim operacija koje podržavaju njegovo poslovanje, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona;
- 2) pouzdani;
- 3) dovoljnog kapaciteta za tačnu obradu podataka neophodnih za obavljanje aktivnosti i blagovremeno pružanje usluga, kao i kapacitet za obradu u uslovima najvećeg opterećenja u pogledu obima naloga, poruka ili transakcija, u skladu sa potrebama, uključujući i u slučaju uvođenja nove tehnologije;

- 4) tehnološki otporni kako bi mogli na adekvatan način odgovoriti na dodatne potrebe za obradom informacija koje nastaju usljed poremećaja na tržištu ili u drugim nepovoljnim situacijama.

Identifikacija i procjena IKT rizika, usluga, sistema i imovine

Član 14

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, identifikuje, klasifikuje i adekvatno dokumentuje sve poslovne funkcije podržane IKT-om, zaduženja i odgovornosti, informacionu imovinu i IKT imovinu koja podržava te funkcije, kao i njihove uloge i međuzavisnosti u pogledu IKT rizika.

(2) Finansijski subjekt je dužan da, po potrebi, a najmanje jednom godišnje, preispituje adekvatnost klasifikacije iz stava 1 ovog člana i cjelokupne pripadajuće dokumentacije.

(3) Finansijski subjekt je dužan da kontinuirano:

- 1) identifikuje sve izvore IKT rizika, a naročito izloženosti riziku prema drugim finansijskim subjektima i od drugih finansijskih subjekata;
- 2) procjenjuje sajber prijetnje i IKT ranjivosti koje se odnose na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu.

(4) Finansijski subjekt je dužan da redovno, a najmanje jednom godišnje, razmatra scenarije rizika koji mogu da utiču na funkcije i imovinu iz stava 3 tačka 2 ovog člana.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da sprovede procjenu rizika u slučaju svake značajne promjene u:

- 1) infrastrukturi mrežnih i informacionih sistema;
- 2) procesima ili procedurama koje utiču na njegove poslovne funkcije podržane IKT-om, informacionu imovinu ili IKT imovinu.

(6) Finansijski subjekt je dužan da identifikuje svu informacionu imovinu i IKT imovinu, uključujući mrežne resurse, hardversku opremu i imovinu na udaljenim lokacijama, i da posebno evidentira informacionu imovinu i IKT imovinu koja se smatra kritičnom.

(7) Finansijski subjekt je dužan da dokumentuje konfiguraciju informacione imovine i IKT imovine i informacije o povezanosti i međuzavisnosti između različite informacione i IKT imovine.

(8) Finansijski subjekt je dužan da identifikuje i dokumentuje sve procese koji zavise od trećih strana koje pružaju IKT usluge, kao i da identifikuje međusobne povezanosti sa trećim stranama koje pružaju IKT usluge kojima se podržavaju kritične ili važne funkcije.

(9) Finansijski subjekt je dužan da, radi postupanja u skladu sa st. 1, 6, 7 i 8 ovog člana, vodi odgovarajuće registre, koje mora da ažurira redovno i u slučaju svake značajne promjene iz stava 5 ovog člana.

(10) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da redovno, a najmanje jednom godišnje, sprovodi procjenu IKT rizika za sve zastarjele IKT sisteme, kao i vanredno prije i nakon povezivanja tehnologija, aplikacija ili sistema.

Zaštita IKT sistema i sprečavanje IKT incidenata

Član 15

(1) Radi adekvatne zaštite IKT sistema i u cilju organizovanja mjera odgovora, finansijski subjekt dužan je da kontinuirano prati i kontroliše bezbjednost i funkcionisanje IKT sistema i alata, kao i da na najmanju moguću mjeru svede uticaj IKT rizika na IKT sisteme, primjenom odgovarajućih IKT bezbjednosnih alata, politika i procedura.

(2) Finansijski subjekt je dužan da osmisli, kreira i/ili nabavi i primijeni politike, procedure, protokole i alate za IKT bezbjednost u cilju obezbjeđivanja otpornosti, kontinuiteta i dostupnosti IKT sistema, a naročito onih koji podržavaju kritične ili važne funkcije, i u cilju održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, bez obzira da li su u stanju mirovanja, upotrebi ili prenosu.

(3) Radi ostvarivanja ciljeva iz stava 2 ovog člana, finansijski subjekt je dužan da koristi IKT rješenja i procese koji su primjereni, u smislu člana 5 ovog zakona i kojima se:

- 1) omogućava bezbjednost sredstava i metoda za prenos podataka;
- 2) na najmanju moguću mjeru svodi rizik od oštećenja ili gubitka podataka, neovlašćenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje;
- 3) sprečava nedostupnost i gubitak podataka, narušavanje autentičnosti, integriteta i povjerljivosti podataka;
- 4) obezbjeđuje zaštitu podataka od rizika koji proizilaze iz upravljanja podacima, uključujući propuste u administraciji, rizike povezane sa obradom i ljudske greške.

(4) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima:

- 1) razvije i usvoji politiku informacione bezbjednosti kojom se utvrđuju pravila za zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, informacione imovine i IKT imovine, uključujući podatke i imovinu njegovih klijenata, kada je to primjenljivo;
- 2) primjenom pristupa zasnovanog na procjeni rizika, uspostavi pouzdanu strukturu za upravljanje mrežom i infrastrukturu, korišćenjem odgovarajućih tehnika, metoda i protokola;
- 3) utvrdi i primjenjuje politike kojima se odobrava fizički i logički pristup informacionoj imovini i IKT imovini do nivoa koji je neophodan za obavljanje opravdanih i odobrenih poslova i aktivnosti, i u tu svrhu primjenjuje skup pravila, postupaka i kontrola za adekvatno upravljanje pravima pristupa i kontrolu pristupa;
- 4) utvrdi i primjenjuje politike i protokole za korišćenje pouzdanih mehanizama provjere autentičnosti, zasnovanih na relevantnim standardima i specijalizovanim sistemima kontrole, kao i mjere za zaštitu kriptografskih ključeva za šifrovanje podataka;
- 5) utvrdi i primjenjuje politike, procedure i kontrole za upravljanje IKT promjenama, uključujući promjene softverskih i hardverskih komponenti, firmvera, sistema i bezbjednosnih parametara, koje su zasnovane na procjeni rizika i predstavljaju sastavni dio opšteg procesa upravljanja promjenama u finansijskom subjektu, kako bi se obezbijedilo da se sve promjene IKT sistema evidentiraju, testiraju, procjenjuju, odobravaju, sprovode i provjeravaju na kontrolisan način;
- 6) utvrdi i primjenjuje odgovarajuće i sveobuhvatne politike za primjenu softverskih i hardverskih zakrpa i ažuriranja.

(5) Finansijski subjekt je dužan da strukturu za upravljanje mrežom i infrastrukturu iz stava 4 tačka 2 ovog člana kreira i implementira na način kojim se omogućava brzo ukidanje ili segmentiranje mrežnog pristupa, kako bi se u najvećoj

mogućoj mjeri ograničilo i spriječilo širenje zaraze, a naročito u slučaju međusobno povezanih finansijskih procesa.

(6) Struktura za upravljanje mrežom i infrastrukturu iz stava 4 tačka 2 ovog člana može da obuhvati primjenu automatizovanih mehanizama za izolaciju zahvaćene informacione imovine u slučaju sajber napada.

(7) Postupak upravljanja IKT promjenama iz stava 4 tačka 5 ovog člana mora biti odobren od strane odgovarajućih linija i nivoa odlučivanja finansijskog subjekta, i mora da se sprovodi u skladu sa posebno utvrđenim protokolima finansijskog subjekta.

Praćenje, otkrivanje i analiza IKT događaja i incidenata

Član 16

(1) Finansijski subjekt je dužan da uspostavi mehanizme za brzo otkrivanje neuobičajenih aktivnosti, u skladu sa članom 22 ovog zakona, uključujući otkrivanje problema u performansama IKT mreže i IKT incidenata, kao i mehanizme za identifikovanje potencijalnih značajnih jedinstvenih tačaka prekida.

(2) Finansijski subjekt je dužan da obezbijedi redovno testiranje mehanizama iz stava 1 ovog člana na način propisan članom 28 ovog zakona.

(3) Mehanizmi iz stava 1 ovog člana moraju da omoguće kontrolu na više nivoa, utvrde pragove za dobijanje upozorenja i kriterijume za aktiviranje i započinjanje procesa odgovora na IKT incidente, što uključuje i mehanizme za automatsko obavješćavanje relevantnih lica zaduženih za odgovor na IKT incidente.

(4) Finansijski subjekt je dužan da obezbijedi dovoljne resurse i kapacitete za praćenje aktivnosti korisnika, otkrivanje neuobičajnih IKT događaja i IKT incidenata, a naročito sajber napada.

(5) Pružalac usluga dostave podataka dužan je da uspostavi sisteme kojima se može efikasno provjeriti da li su izvještaji o trgovanju potpuni i kojima se mogu utvrditi propusti i očigledne greške i zahtijevati ponovni prenos tih izvještaja.

Kontinuitet poslovanja, odgovor na IKT incidente i oporavak nakon njih

Član 17

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na osnovu rezultata postupanja u skladu sa članom 14 ovog zakona, uspostavi sveobuhvatnu IKT politiku kontinuiteta poslovanja.

(2) IKT politika kontinuiteta poslovanja iz stava 1 ovog člana predstavlja sastavni dio opšte politike kontinuiteta poslovanja finansijskog subjekta, a može se usvojiti u formi zasebnog, namjenskog akta.

(3) Finansijski subjekt je dužan da IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana primjenjuje pomoću odgovarajućih, namjenskih i dokumentovanih mjera, planova, procedura i mehanizama u cilju:

- 1) obezbjeđivanja kontinuiteta kritičnih ili važnih funkcija finansijskog subjekta;
- 2) brzog, adekvatnog i efikasnog odgovora na sve IKT incidente i njihovog rješavanja, na način kojim se ograničava šteta i daje prioritet nastavku poslovanja i oporavku;
- 3) pokretanja, bez odlaganja, namjenskih planova kojima se, za sve vrste IKT incidenata, omogućava sprovođenje njima prilagođenih mjera, procesa i

tehnologija za suzbijanje negativnih efekata i sprečavanje nastanka dalje štete, kao i posebno prilagođenih procedura za odgovor i oporavak iz člana 18 ovog zakona;

4) preliminarne procjene uticaja, štete i gubitaka;

5) utvrđivanja mjera za komunikaciju i upravljanje u kriznim situacijama kojima se obezbjeđuje dostavljanje ažurnih informacija svim relevantnim zaposlenima i eksternim zainteresovanim stranama u skladu sa članom 20 ovog zakona, i za izvještavanje nadležnog organa u skladu sa odredbama člana 24 ovog zakona.

(4) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje odgovarajuće planove za odgovor i oporavak u IKT oblasti.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi nezavisnu internu reviziju planova iz stava 4 ovog člana.

(6) Finansijski subjekt dužan je da uspostavi, održava i periodično testira odgovarajuće IKT planove kontinuiteta poslovanja, naročito za kritične ili važne funkcije koje, na osnovu zaključenih ugovora, obavljaju ili isporučuju treće strane koje pružaju IKT usluge.

(7) Finansijski subjekt je dužan da, u okviru opšte politike kontinuiteta poslovanja, sprovodi analizu uticaja na poslovanje odnosno analizu svoje izloženosti ozbiljnim poremećajima u poslovanju.

(8) Finansijski subjekt je dužan da, u okviru analize uticaja na poslovanje iz stava 7 ovog člana, na osnovu kvalitativnih i kvantitativnih kriterijuma, korišćenjem raspoloživih internih i eksternih podataka i analize scenarija, procijeni potencijalni uticaj ozbiljnih poremećaja u poslovanju.

(9) Finansijski subjekt je dužan da prilikom vršenja analize uticaja na poslovanje iz stava 7 ovog člana uzme u obzir kritičnost identifikovanih poslovnih funkcija, pomoćnih procesa, informacione imovine, zavisnosti od trećih strana, kao i njihovu povezanost i međuzavisnost.

(10) Finansijski subjekt je dužan da osmisli i koristi IKT imovinu i IKT usluge na način koji je u potpunosti usklađen sa rezultatima analize uticaja na poslovanje iz stava 7 ovog člana, naročito u pogledu obezbjeđivanja adekvatne redundanse svih kritičnih komponenti.

(11) Redundansa, u smislu stava 10 ovog člana, označava postojanje jedne ili više dodatnih komponenti koje preuzimaju funkciju primarne komponente u slučaju njenog prekida rada.

(12) U okviru sveobuhvatnog upravljanja IKT rizicima, finansijski subjekt dužan je da:

1) za IKT sisteme koji podržavaju funkcije finansijskog subjekta, testira planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana i IKT planove kontinuiteta poslovanja iz stava 6 ovog člana:

- najmanje jednom godišnje; i
- u slučaju značajnih promjena IKT sistema koji podržavaju kritične ili važne funkcije finansijskog subjekta.

2) testira planove komunikacije u kriznim situacijama iz člana 20 ovog zakona.

(13) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da testiranjem iz stava 12 tačka 1 ovog člana obuhvati scenarije sajber napada i scenarije prelazaka između primarne IKT infrastrukture i rezervnih kapaciteta, rezervnih

kopija podataka, rezervnih sistema i rezervnih lokacija, neophodnih za ispunjavanje zahtjeva iz člana 18 ovog zakona.

(14) Finansijski subjekt je dužan da redovno preispituje IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana i planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana, uzimajući u obzir rezultate testiranja iz stava 12 ovog člana, preporuke revizije i zahtjeve nadležnog organa.

(15) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi odgovorno lice ili organizacionu jedinicu za upravljanje kriznim situacijama koja je, u slučaju pokretanja planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, naročito dužna da utvrdi jasne procedure za upravljanje internom i eksternom komunikacijom u skladu sa članom 20 ovog zakona.

(16) U slučaju pokretanja IKT planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, finansijski subjekt je dužan da vodi evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna.

(17) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi procjenu ukupnih godišnjih troškova i gubitaka koje su prouzrokovali značajni IKT incidenti.

(18) Centralno klirinško depozitarno društvo dužno je da dostavlja Komisiji kopije rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi.

Politike i procedure za izradu rezervnih kopija podataka i procedure i metode za ponovno uspostavljanje i oporavak

Član 18

(1) Kako bi se omogućilo ponovno uspostavljanje IKT sistema i povratak podataka uz minimalno trajanje prekida i ograničili poremećaji u radu i gubici, finansijski subjekt dužan je da, u okviru sistema upravljanja IKT rizicima, razvije i usvoji:

- 1) politike i procedure kojima se, na osnovu kritičnosti informacija i povjerljivosti podataka, utvrđuju obim i minimalna učestalost izrade rezervnih kopija podataka;
- 2) procedure i metode za povratak, ponovno uspostavljanje i oporavak.

(2) Finansijski subjekt je dužan da obezbijedi sisteme za izradu rezervnih kopija podataka koji se mogu koristiti u skladu sa politikama i procedurama za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i u skladu sa procedurama i metodama za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana.

(3) Korišćenjem sistema za izradu rezervnih kopija podataka iz stava 2 ovog člana ne smije se ugroziti bezbjednost mrežnih i informacionih sistema ni dostupnost, autentičnost, integritet ili povjerljivost podataka.

(4) Finansijski subjekt je dužan da periodično testira procedure za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i procedure i metode za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana.

(5) Kada finansijski subjekt koristi sopstvene sisteme za povratak podataka iz rezervnih kopija, dužan je da obezbijedi da se za te potrebe koriste IKT sistemi koji su fizički i logički odvojeni od izvornih IKT sistema iz kojih podaci potiču.

(6) IKT sistemi iz stava 5 ovog člana koji su namijenjeni za oporavak, moraju biti bezbjedno zaštićeni od neovlašćenog pristupa i IKT kompromitacija i omogućiti blagovremeno ponovno uspostavljanje usluga, pri čemu se, po potrebi, koriste rezervne kopije podataka i sistema.

(7) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da održava rezervne IKT kapacitete koji imaju resurse, sposobnosti i funkcije dovoljne za adekvatno obezbjeđivanje potreba poslovnih procesa.

(8) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da, u skladu sa svojim rizičnim profilom, procijeni potrebu održavanja rezervnih IKT kapaciteta iz stava 7 ovog člana.

(9) Finansijski subjekat je dužan da, prilikom određivanja ciljnog vremena oporavka i ciljne tačke oporavka za svaku funkciju, uzme u obzir značaj te funkcije, a naročito da li se radi o kritičnoj ili važnoj funkciji, kao i potencijalni ukupni uticaj ciljeva oporavka na efikasnost tržišta.

(10) Ciljno vrijeme oporavka i ciljna tačka oporavka iz stava 9 ovog člana moraju biti takvi da, u ekstremnim scenarijima, obezbjeđuju ispunjavanje dogovorenih nivoa usluga.

(11) Prilikom oporavka od IKT incidenta, finansijski subjekt je dužan da sprovede sve neophodne kontrole, uključujući višestruke provjere i usklađivanja, kako bi obezbijedio održavanje najvišeg nivoa integriteta podataka.

(12) Kontrole iz stava 11 ovog člana moraju se sprovoditi i prilikom rekonstrukcije podataka iz eksternih izvora, radi obezbjeđivanja usklađenosti svih podataka između sistema.

(13) Centralna druga ugovorena strana dužna je da uspostavi planove koji moraju omogućiti oporavak svih transakcija koje su bile u toku u trenutku nastanka poremećaja, kako bi se obezbijedio nesmetan i siguran nastavak poslovanja centralne druge ugovorne strane i omogućilo izvršenje obaveze na predviđeni datum.

(14) Pružalac usluga dostave podataka dužan je da obezbijedi odgovarajuće resurse i infrastrukturu za izradu rezervnih kopija i obnovu sistema, radi kontinuiranog pružanja i održavanja svojih usluga.

(15) Centralno klirinško depozitarno društvo dužno je održavati najmanje jedno sekundarno mjesto obrade, opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem, kako bi se zadovoljile poslovne potrebe.

(16) Sekundarno mjesto obrade iz stava 15 ovog člana:

- 1) mora biti geografski udaljeno od primarnog mjesta obrade kako bi se osigurao različit profil rizika i spriječilo da bude pogođeno istim događajem koji je zahvatio primarno mjesto;
- 2) mora omogućavati kontinuitet kritičnih ili važnih funkcija na način identičan primarnom mjestu ili pružati nivo usluga potreban za izvršenje ključnih operacija finansijskog subjekta u skladu sa ciljevima oporavka;
- 3) mora biti odmah dostupno osoblju finansijskog subjekta kako bi se osigurao kontinuitet kritičnih ili važnih funkcija u slučaju nedostupnosti primarnog mjesta obrade.

Usavršavanje u cilju jačanja digitalne operativne otpornosti

Član 19

(1) Finansijski subjekt je dužan da obezbijedi kapacitete i odredi lica zadužena za prikupljanje informacija o ranjivostima, sajber prijetnjama, IKT incidentima, a naročito o sajber napadima, kao i za analizu njihovog mogućeg uticaja na digitalnu operativnu otpornost finansijskog subjekta.

(2) Finansijski subjekt je dužan da uspostavi proces naknadne analize IKT incidenata, koji se sprovodi nakon što značajan IKT incident poremeti obavljanje njegovih osnovnih aktivnosti, u cilju analize uzroka poremećaja i utvrđivanja potrebnih poboljšanja u IKT operacijama ili u IKT politici kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona.

(3) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi informacije o izmjenama koje su sprovedene nakon analize IKT incidenta iz stava 2 ovog člana.

(4) Naknadnom analizom IKT incidenta iz stava 2 ovog člana mora se utvrditi da li su uspostavljene procedure bile ispoštovane i da li su preduzete mjere bile djelotvorne, uključujući:

- 1) brzinu reagovanja na bezbjednosna upozorenja i utvrđivanja uticaja IKT incidenta i njegove ozbiljnosti;
- 2) kvalitet i brzinu sprovođenja forenzičke analize, u slučajevima kada je to svrsishodno;
- 3) efikasnost interne eskalacije incidenta;
- 4) efikasnost interne i eksterne komunikacije.

(5) Finansijski subjekt je dužan da obezbijedi da se iskustva stečena kroz testiranje digitalne operativne otpornosti iz čl. 27 do 32 ovog zakona, kao i iz nastalih IKT incidenata, a naročito sajber napada, saznanja o izazovima koji su se pojavili prilikom pokretanja planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona, relevantne informacije dobijene od drugih subjekata, kao i informacije u vezi sa zahtjevima nadležnog organa, blagovremeno, adekvatno i kontinuirano koriste u okviru procesa procjene IKT rizika.

(6) Finansijski subjekt je dužan da iskustva, saznanja i informacije iz stava 5 ovog člana, na odgovarajući način, uzme u obzir prilikom preispitivanja relevantnih komponenti sistema upravljanja IKT rizicima.

(7) Finansijski subjekt je dužan da prati efikasnost sprovođenja strategije digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona.

(8) Finansijski subjekt je dužan da evidentira i prati promjenu ukupnog profila IKT rizika tokom vremena, analizira učestalost, vrste, razmjere i trendove IKT incidenata, a naročito sajber napada i njihovih obrazaca, kako bi razumio nivo svoje izloženosti IKT riziku, posebno u odnosu na kritične ili važne funkcije i unaprijedio stepen svoje zrelosti i spremnosti u oblasti sajber bezbjednosti.

(9) Finansijski subjekt je dužan da obezbijedi da viši IKT kadar, najmanje jednom godišnje, podnosi izvještaj organu upravljanja o zaključcima izvedenim iz iskustava, saznanja i informacija iz stava 5 ovog člana, sa predlozima za dalje postupanje.

(10) Finansijski subjekt je dužan da osmisli i sprovodi programe za podizanje svijesti o IKT bezbjednosti i obuke o digitalnoj operativnoj otpornosti, kao obavezne djelove svojih programa obuke zaposlenih.

(11) Programi i obuke iz stava 10 ovog člana primjenjuju se na sve zaposlene i članove višeg rukovodstva, a nivo njihove složenosti mora biti prilagođen nadležnostima i poslovima koje ta lica obavljaju.

(12) Finansijski subjekt je dužan da, kada je to primjenljivo, uključi treće strane koje pružaju IKT usluge u odgovarajuće programe obuke, u skladu sa članom 38 stav 3 tačka 11 ovog zakona.

(13) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da kontinuirano prati trendove u razvoju tehnologija, kako bi bolje razumio mogući uticaj primjene novih tehnologija na zahtjeve u oblasti IKT bezbjednosti i digitalnu operativnu otpornost.

(14) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da bude upoznat sa najnovijim metodama za upravljanje IKT rizicima, kako bi mogao efikasno da odgovori na postojeće i nove oblike sajber napada.

Komunikacija u kriznim situacijama

Član 20

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi planove komunikacije u kriznim situacijama, koji omogućavaju da na odgovoran način saopštava informacije, najmanje o značajnim IKT incidentima i značajnim ranjivostima, klijentima, poslovnim partnerima i široj javnosti, u zavisnosti od slučaja.

(2) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje politike komunikacije za zaposlene i sa eksternim zainteresovanim stranama.

(3) Politike komunikacije iz stava 2 ovog člana, u dijelu koji se odnosi na zaposlene, moraju uzeti u obzir da se mora praviti razlika između zaposlenih koje je potrebno samo informisati i zaposlenih koji učestvuju u upravljanju IKT rizicima, odnosno koji su zaduženi za odgovor i oporavak.

(4) Najmanje jedno lice u finansijskom subjektu mora biti zaduženo za sprovođenje strategije komunikacije u slučaju IKT incidenata i da, u tu svrhu, obavlja poslove informisanja medija i javnosti.

Pojednostavljeni sistem upravljanja IKT rizicima

Član 21

(1) Odredbe čl. 8 do 19 ovog zakona ne primjenjuju se na malo i nepovezano investiciono društvo i malu instituciju za profesionalnu penzionu štednju.

(2) Finansijski subjekti iz stava 1 ovoga člana dužni su da:

- 1) uspostave i održavaju pouzdan i dokumentovan sistem upravljanja IKT rizikom, koji detaljno opisuje mehanizme i mjere usmjerene na brzo, efikasno i sveobuhvatno upravljanje IKT rizikom, uključujući i zaštitu relevantnih fizičkih komponenti i infrastrukture;
- 2) kontinuirano prate bezbjednost i funkcionisanje svih IKT sistema;

- 3) minimiziraju uticaj IKT rizika korišćenjem pouzdanih, otpornih i ažurnih IKT sistema, protokola i alata koji su primjereni za podršku obavljanju njihovih aktivnosti i pružanju usluga, kao i za adekvatnu zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka u mrežnim i informacionim sistemima;
- 4) omoguće pravovremeno identifikovanje izvora IKT rizika i anomalija u mrežnim i informacionim sistemima, kao i brzo postupanje u slučaju IKT incidenata;
- 5) identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge;
- 6) obezbijede kontinuitet kritičnih ili važnih funkcija pomoću planova kontinuiteta poslovanja i mjera odgovora i oporavka, koje uključuju najmanje mjere izrade rezervnih kopija podataka i povraćaja podataka iz rezervnih kopija;
- 7) redovno testiraju efikasnost kontrola koje se sprovode u skladu sa tač. 1 i 3, kao i planove i mjere iz tačke 6 ovog stava;
- 8) u skladu sa potrebama i profilom IKT rizika, koriste relevantne operativne zaključke koji proizlaze iz testiranja iz tačke 7 ovog stava i analiza nakon incidenata u procesu procjene IKT rizika, kao i da razvijaju programe za podizanje svijesti o IKT bezbjednosti i obuke iz oblasti digitalne operativne otpornosti za zaposlene i rukovodstvo.

III. UPRAVLJANJE, KLASIFIKACIJA I IZVJEŠTAVANJE O IKT INCIDENTIMA

Proces upravljanja IKT incidentima

Član 22

(1) Finansijski subjekt je dužan da definiše, uspostavi i primijeni proces upravljanja IKT incidentima radi otkrivanja, upravljanja i obavještanja o IKT incidentima.

(2) Finansijski subjekt je dužan da evidentira sve IKT incidente i ozbiljne sajber prijetnje.

(3) Finansijski subjekt je dužan da uspostavi adekvatne procedure i postupke kojima se obezbjeđuje da se, na dosljedan i objedinjen način postupa sa IKT incidentima, vrši njihovo praćenje i preduzimaju dalje mjere, kako bi se obezbijedilo da se osnovni uzroci IKT incidenata identifikuju, dokumentuju i tretiraju, radi sprečavanja ponavljanja takvih incidenata.

(4) Finansijski subjekt je dužan da, u okviru procesa upravljanja IKT incidentima iz stava 1 ovog člana:

- 1) uspostavi indikatore ranog upozorenja;
- 2) uspostavi procedure za identifikaciju, praćenje, evidentiranje, kategorizaciju i klasifikaciju IKT incidenata prema njihovom prioritetu i nivou ozbiljnosti, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona, uzimajući u obzir kritičnost usluga zahvaćenih incidentom;
- 3) dodijeli zaduženja i odgovornosti za postupanje u slučaju različitih IKT incidenata, prema njihovim vrstama i scenarijima;
- 4) utvrdi planove za komunikaciju sa zaposlenima, eksternim zainteresovanim stranama i medijima u skladu sa članom 20 ovog zakona, planove za obavještanje klijenata, za postupke interne eskalacije incidenata, uključujući prigovore klijenata povezane sa IKT-om, kao i za informisanje drugih finansijskih subjekata sa kojima ima poslovnu saradnju, kada je to primjenljivo;

- 5) obezbijedi da se više rukovodstvo i organ upravljanja izvještavaju najmanje o značajnim IKT incidentima, uz obrazloženje njihovog uticaja, odgovora na njih i dodatnih kontrola koje je potrebno uspostaviti zbog nastanka takvih IKT incidenata;
- 6) uspostavi procedure za odgovor na IKT incidente, kako bi ublažio njihov uticaj i obezbijedio da usluge zahvaćene incidentom ponovo, blagovremeno postanu dostupne, funkcionalne i bezbjedne.

Klasifikacija IKT incidenata i sajber prijetnji

Član 23

(1) Finansijski subjekt je dužan da klasifikuje IKT incidente i da utvrdi njihov uticaj na osnovu sljedećih kriterijuma:

- 1) broja i/ili značaja klijenata zahvaćenih IKT incidentom, ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana zahvaćena incidentom i, kada je to primjenljivo, vrijednosti ili broja transakcija zahvaćenih incidentom, kao i činjenice da li je incident narušio ugled finansijskog subjekta;
- 2) trajanja IKT incidenta, uključujući period prekida pružanja usluge;
- 3) geografske rasprostranjenosti u smislu područja koje je IKT incident zahvatio, naročito ako je zahvatio više od dvije države članice;
- 4) gubitka svojstva podataka usljed IKT incidenta, odnosno gubitka dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka;
- 5) kritičnosti usluga zahvaćenih incidentom, uključujući u pogledu transakcija i operacija finansijskog subjekta;
- 6) ekonomskog uticaja IKT incidenta, odnosno direktnih i indirektnih troškova i gubitaka, u apsolutnom i relativnom smislu.

(2) Finansijski subjekt je dužan da klasifikuje sajber prijetnje kao ozbiljne na osnovu kritičnosti usluga koje su izložene riziku, uključujući u pogledu transakcija i operacija finansijskog subjekta, broja i/ili značaja klijenata izloženih tom riziku ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana izložena tom riziku i geografske rasprostranjenosti u smislu područja izloženih riziku.

Izveštavanje o značajnim IKT incidentima i obavještavanje o ozbiljnim sajber prijetnjama

Član 24

(1) Finansijski subjekt je dužan da o značajnom IKT incidentu izvještava nadležni organ.

(2) Radi izvještavanja iz stava 1 ovog člana, finansijski subjekt je dužan da prikupi i analizira sve relevantne informacije o značajnom IKT incidentu, pripremi dokumentaciju iz stava 3 ovog člana i dostavi je nadležnom organu na način i u roku utvrđenom posebnim propisom nadležnog organa.

(3) Finansijski subjekt je dužan da nadležnom organu dostavi:

- 1) početno obavještenje;
- 2) prelazni izvještaj nakon početnog obavještenja iz tačke 1 ovog stava, čim dođe do značajne promjene u statusu prijavljenog značajnog IKT incidenta ili promjene u postupanju sa tim incidentom u skladu sa novim dostupnim informacijama, a nakon toga, po potrebi, ažurirane prelazne izvještaje u slučaju bitne promjene statusa incidenta, kao i na izričit zahtjev nadležnog organa;

3) završni izvještaj, nakon što izvrši analizu osnovnog uzroka incidenta, bez obzira na to da li su mjere za ublažavanje njegovog uticaja već sprovedene, i kada su dostupni konačni podaci o uticaju incidenta, a kojima se mogu zamijeniti prethodne procjene.

(4) Dokumentacija iz stava 3 ovog člana mora sadržati sve informacije koje su nadležnom organu potrebne da utvrdi ozbiljnost značajnog IKT incidenta i procijeni mogućnost prekograničnog uticaja tog incidenta.

(5) Izuzetno od stava 2 ovog člana, u slučaju da finansijski subjekt zbog tehničkih poteškoća nije u mogućnosti da dostavi početno obavještenje iz stava 3 ovog člana na način utvrđen posebnim propisom nadležnog organa, dostavljanje se može izvršiti na drugi pogodan način.

(6) Finansijski subjekt može da obavijesti nadležni organ o ozbiljnoj sajber prijetnji kada procijeni da je prijetnja relevantna za finansijski sistem, korisnike usluga ili klijente.

(7) Nadležni organ može da dostavi informacije o ozbiljnoj sajber prijetnji iz stava 6 ovog člana organima iz stava 11 ovog člana.

(8) Kada nastane značajan IKT incident koji utiče na finansijske interese klijenata, finansijski subjekt dužan je da, bez odlaganja, odmah po saznanju za takav incident, obavijesti klijente o tom incidentu i o mjerama preduzetim za ublažavanje negativnih uticaja tog incidenta.

(9) U slučaju ozbiljne sajber prijetnje, finansijski subjekt je dužan da, kada je to primjenljivo, obavijesti klijente na koje bi ta prijetnja mogla da utiče o mjerama zaštite koje mogu da preduzmu.

(10) Finansijski subjekt može, u skladu sa zakonom, da povjeri trećoj strani obavljanje poslova obavješćavanja u skladu sa ovim članom, pri čemu je taj finansijski subjekt odgovoran za usklađenost sa odredbama ovog člana.

(11) Po prijemu početnog obavješćenja i svakog izvještaja iz stava 3 ovog člana, nadležni organ blagovremeno dostavlja podatke o značajnom IKT incidentu, kada je to primjenljivo, a u skladu sa njihovim nadležnostima:

- 1) EBA-i, ESMA-i ili EIOPA-i;
- 2) ECB-u, u slučaju finansijskih subjekata iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona;
- 3) organu koji je, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, nadležan za zaštitu finansijskog subjekta od sajber prijetnji i incidenata;
- 4) organu koji je, u skladu sa zakonom kojim se uređuje sanacija kreditnih institucija, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje kritičnih funkcija u smislu tog zakona;
- 5) organu koji je, u skladu sa zakonom kojim se uređuje sanacija investicionih društava, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje ključnih funkcija u smislu tog zakona;
- 6) drugom javnom organu, u skladu sa zakonom.

(12) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om, EIOPA-om i/ili ECB-om u postupku iz člana 19 stav 7 Regulative (EU) br. 2022/2554, koji ti organi sprovode radi procjene relevantnosti značajnog IKT incidenta za nadležne organe u drugim državama članicama, u skladu sa kriterijumima iz člana 11 Regulative (EU) br. 2024/1772.

(13) U slučaju da, u skladu sa članom 19 stav 7 Regulative (EU) br. 2022/2554, putem ESCB-a primi obavješćenje od ECB-a o pitanjima koja su od značaja za platni

sistem, Centralna banka za finansijski subjekt iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona, kada je to primjenljivo, preduzima sve neophodne mjere za zaštitu stabilnosti finansijskog sistema.

(14) Komisija obavještava relevantni nadležni organ države članice domaćina o značajnom IKT incidentu u slučaju kada Centralno klirinško depozitarno društvo ima značajnu prekograničnu aktivnost u toj državi članici domaćina, kada je vjerovatno da će značajni IKT incident imati ozbiljne posljedice po finansijska tržišta države članice domaćina, kao i u situacijama u kojima postoje aranžmani o saradnji među nadležnim organima u vezi sa nadzorom finansijskih subjekata.

Povratne informacije nadležnog organa

Član 25

(1) Nadležni organ je dužan da po prijemu dokumentacije iz člana 24 stav 3 ovog zakona, finansijskom subjektu potvrdi prijem.

(2) Po prijemu početnog obavještenja i svakog izvještaja iz člana 24 stav 3 ovog zakona, nadležni organ može, kada je to moguće, finansijskom subjektu blagovremeno pružiti relevantne i srazmjerne informacije ili opšte smjernice za dalje postupanje, naročito davanjem na uvid svih relevantnih anonimizovanih informacija i saznanja o sličnim prijetnjama, kao i da sa tim finansijskim subjektom razmotri primijenjene korektivne mjere, načine za ublažavanje i umanjenje negativnih uticaja značajnog IKT incidenta na finansijski sektor u cjelini.

(3) Aktivnostima nadležnog organa iz stava 2 ovog člana ne dovode se u pitanje tehnički doprinosi, smjernice, korektivne mjere i dalja postupanja koja, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, pružaju i sprovode organi određeni tim zakonom.

(4) U slučaju iz stava 2 ovog člana, finansijski subjekt je u potpunosti odgovoran za postupanje sa značajnim IKT incidentom i za njegove posljedice.

Operativni i sigurnosni incidenti povezani sa plaćanjem

Član 26

Finansijski subjekti iz člana 2 stav 1 tač. 1 do 4 ovog zakona, dužni su da u slučaju operativnih i sigurnosnih incidenata povezanih sa plaćanjem, uključujući i značajne operativne i sigurnosne incidente povezane sa plaćanjem, shodno primjenjuju odredbe čl. 22 do 25 ovog zakona.

IV. TESTIRANJE DIGITALNE OPERATIVNE OTPORNOSTI

Opšti zahtjevi za sprovođenje testiranja digitalne operativne otpornosti

Član 27

(1) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, a u cilju procjene spremnosti za upravljanje IKT incidentima, identifikovanja slabosti, nedostataka i odstupanja u digitalnoj operativnoj otpornosti i blagovremenog sprovođenja korektivnih mjera, da uspostavi, održava i redovno preispituje program za testiranje digitalne operativne otpornosti.

(2) Program za testiranje digitalne operativne otpornosti iz stava 1 ovog člana, kao dio okvira za upravljanje IKT rizicima, mora biti efikasan i sveobuhvatan i sadržati niz procjena, testova, metodologija, praksi i alata koji se sprovode i primjenjuju u skladu sa čl. 28 do 31 ovog zakona.

(3) Finansijski subjekt iz stava 1 ovog člana, dužan je da sprovodi program za testiranje digitalne operativne otpornosti primjenom pristupa zasnovanog na procjeni rizika, pri čemu mora voditi računa o promjenljivom karakteru IKT rizika, konkretnim rizicima kojima je izložen ili bi mogao biti izložen, kritičnosti informacione imovine i usluga, kao i o svim drugim relevantnim faktorima.

(4) Finansijski subjekt je dužan da obezbijedi da testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode nezavisna interna ili eksterna lica.

(5) U slučaju kada testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode interna lica, finansijski subjekt je dužan da za te potrebe obezbijedi dovoljne resurse i preduzme mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja tog testiranja.

(6) Finansijski subjekt iz stava 1 ovog člana, dužan je da uspostavi politike i procedure za određivanje prioriteta, klasifikacije i otklanjanje svih problema otkrivenih tokom testiranja digitalne operativne otpornosti, kao i metodologije za internu provjeru radi dobijanja potvrde da su sve identifikovane slabosti, nedostaci i odstupanja u potpunosti otklonjeni.

(7) Finansijski subjekt iz stava 1 ovog člana, dužan je da najmanje jednom godišnje, sprovodi adekvatne testove svih IKT sistema i aplikacija koje podržavaju kritične ili važne funkcije tog finansijskog subjekta.

Testiranje IKT alata i sistema

Član 28

(1) Programom za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona mora se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, obezbijediti sprovođenje odgovarajućih testova, kao što su:

- 1) procjene i skeniranja ranjivosti;
- 2) analize javno dostupnih izvora;
- 3) procjene bezbjednosti mreže;
- 4) analize odstupanja;
- 5) preispitivanja fizičke bezbjednosti;
- 6) upitnici i softverska rješenja za skeniranje;
- 7) pregledi izvornog koda, kada je to izvodljivo;
- 8) testiranja zasnovana na scenarijima;
- 9) testiranja kompatibilnosti;
- 10) testiranja performansi;
- 11) testiranja od kraja do kraja (*eng. end-to-end*), odnosno kroz sve faze rada;
- 12) penetraciona testiranja.

(2) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt, dužan je da testiranja iz stava 1 ovog člana sprovodi primjenom pristupa zasnovanog na procjeni rizika u skladu sa strateškim planiranjem testiranja u IKT oblasti, uzimajući u obzir potrebu za održavanje uravnoteženog pristupa između obima resursa i vremena potrebnog za sprovođenje testiranja u IKT oblasti, sa jedne strane, i hitnosti, vrste rizika, kritičnosti

informacione imovine i usluga, kao i drugih relevantnih faktora, uključujući sposobnost tog finansijskog subjekta da preuzme proračunate rizike, sa druge strane.

(3) Centralno klirinško depozitarno društvo i Centralna druga ugovorna strana, dužni su da sprovode procjene ranjivosti prije svake primjene ili ponovne primjene novih ili postojećih aplikacija, infrastrukturnih komponenti i IKT usluga koje podržavaju kritične ili važne funkcije finansijskog subjekta.

Napredno testiranje IKT alata, sistema i procesa zasnovano na TLPT-u

Član 29

(1) Finansijski subjekt iz stava 4 ovog člana, dužan je da sprovodi napredno testiranje u formi penetracionog testiranja vođenog prijetnjama (u daljem tekstu: TLPT), najmanje jednom u tri godine.

(2) Izuzetno od stava 1 ovog člana, nadležni organ može, uzimajući u obzir rizični profil finansijskog subjekta i operativne okolnosti, da finansijskom subjektu utvrdi obavezu promijene učestalosti naprednog testiranja.

(3) TLPT iz stava 1 ovog člana mora obuhvatiti više kritičnih ili važnih funkcija finansijskog subjekta ili sve takve funkcije, i sprovodi se na produkcionim sistemima koji podržavaju te funkcije.

(4) Nadležni organ određuje finansijske subjekte, koji nisu klasifikovani kao mikro finansijski subjekti i nisu subjekti iz člana 21 stav 1 ovog zakona, koji su dužni da sprovode TLPT iz stava 1 ovog člana, uzimajući u obzir princip proporcionalnosti iz člana 5 ovog zakona, na osnovu procjene:

- 1) uticaja aktivnosti i usluga finansijskog subjekta na finansijski sektor;
- 2) mogućih rizika po finansijsku stabilnost, uzimajući u obzir sistemski značaj finansijskog subjekta na:
 - nacionalnom nivou;
 - nivou Evropske unije, kada je to primjenljivo.
- 3) profila IKT rizika finansijskog subjekta, nivoa njegove zrelosti u IKT oblasti i karakteristika tehnologije koju koristi.

(5) Nadležni organ može izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, iz ovog člana i čl. 30 do 32 ovog zakona, da povjeri drugom nadležnom organu, osim određivanja finansijskih subjekata koji su dužni da sprovode TLPT.

(6) Za potrebe planiranja i sprovođenja TLPT-a iz stava 1 ovog člana, finansijski subjekt je dužan da:

- 1) utvrdi sve relevantne IKT sisteme, procese i tehnologije kojima se podržavaju IKT usluge i kritične ili važne funkcije, uključujući i one kojima se podržavaju kritične ili važne funkcije koje obavljaju ili isporučuju treće strane koje pružaju IKT usluge;
- 2) procijeni koje kritične ili važne funkcije treba da budu obuhvaćene TLPT-om; i
- 3) u skladu sa procjenom iz tačke 2 ovog stava, precizno definiše planirani obim TLPT-a, kao i da rezultate procjene dostavi nadležnom organu.

(7) Nadležni organ prati sve faze pripreme i sprovođenja TLPT-a i odobrava njegove ključne elemente, uključujući i planirani obim TLPT-a iz stava 6 tačka 3 ovog člana, ukoliko procijeni da su ispunjeni uslovi za sprovođenje adekvatnog i efikasnog testiranja.

Učešće treće strane koja pruža IKT usluge u TLPT-u

Član 30

(1) U slučaju kada je treća strana koja pruža IKT usluge obuhvaćena TLPT-om, finansijski subjekt je dužan da preduzme neophodne mjere i zaštitne mehanizme u skladu sa kojima se obezbjeđuje učešće tih trećih strana u TLPT-u, pri čemu ostaje odgovoran za usklađenost sa ovim zakonom.

(2) Ako se opravdano može očekivati da će učešće treće strane koja pruža IKT usluge u TLPT-u, u skladu sa stavom 1 ovog člana, negativno uticati na kvalitet ili bezbjednost usluga koje ta treća strana pruža klijentima koji nisu finansijski subjekti iz člana 2 ovog zakona, ili na povjerljivost podataka povezanih sa tim uslugama, finansijski subjekt može sa tom trećom stranom zaključiti sporazum kojim se toj trećoj strani omogućava da direktno zaključi ugovor sa eksternim licem koje vrši testiranje, radi sprovođenja objedinjenog TLPT-a kojim je obuhvaćeno više finansijskih subjekata kojima ta treća strana pruža IKT usluge (u daljem tekstu: objedinjeni TLPT), pod koordinacijom jednog odabranog finansijskog subjekta.

(3) Objedinjeni TLPT mora obuhvatiti relevantan opseg IKT usluga kojima se podržavaju kritične ili važne funkcije koje su finansijski subjekti ugovorili sa trećom stranom koja pruža IKT usluge.

(4) Ne dovodeći u pitanje zahtjeve iz člana 29 st. 3 i 6 ovog zakona, objedinjeni TLPT se, u smislu člana 29 stav 1 ovog zakona, smatra TLPT-om koji je sproveo finansijski subjekt obuhvaćen tim testiranjem.

(5) Broj finansijskih subjekata koji učestvuju u objedinjenom TLPT-u mora biti prilagođen složenosti i vrsti usluga obuhvaćenih tim testiranjem.

(6) Finansijski subjekt je dužan da, u saradnji sa trećim stranama koje pružaju IKT usluge, drugim uključenim stranama i licima koja sprovode testiranje, osim nadležnog organa, primijeni efikasne kontrole upravljanja rizicima radi ublažavanja rizika od mogućih negativnih uticaja na podatke, oštećenja imovine i poremećaja u obavljanju kritičnih ili važnih funkcija, usluga i operacija kod samog finansijskog subjekta, drugih finansijskih subjekata sa kojima ima poslovnu saradnju, kao i u finansijskom sektoru.

Izveštavanje o TLPT-u i međusoba saradnja nadležnih organa u TLPT-u

Član 31

(1) Po završetku TLPT-a, nakon usaglašavanja izvještaja i planova za otklanjanje utvrđenih nedostataka, finansijski subjekt i, kada je to primjenljivo, eksterna lica koja su sprovele TLPT, dužni su da nadležnom organu, odnosno nadležnom organu kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona, dostave rezime relevantnih nalaza, planove za otklanjanje utvrđenih nedostataka i dokumentaciju kojom se potvrđuje da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona.

(2) Nadležni organ iz stava 1 ovog člana, finansijskom subjektu izdaje potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, kada se to može utvrditi iz dostavljene dokumentacije.

(3) Izuzetno od stava 2 ovog člana, potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, izdaje:

- 1) nadležni organ koji je vodio TLPT, kada je više nadležnih organa učestvovalo u testiranju;
- 2) TLPT organ druge države članice, kada je TLPT vodio taj organ.

(4) Za potrebe sprovođenja TLPT-a kod finansijskog subjekta koji pruža usluge u više država članica, uključujući i preko filijala, kao i sprovođenja zajedničkog TLPT-a i objedinjenog TLPT-a u slučaju kada treća strana koja pruža IKT usluge pruža IKT usluge finansijskim subjektima u više država članica, nadležni organ sarađuje sa TLPT organima drugih država članica u skladu sa odredbama člana 16 Regulative (EU) br. 2025/1190.

(5) U slučaju kada je potvrdu o sprovedenom testiranju izdao organ koji nije zadužen za nadzor finansijskog subjekta, taj finansijski subjekt je dužan da obavijesti svoj nadležni organ o dobijanju te potvrde, i uz obavještenje dostavi rezime relevantnih nalaza i planove za otklanjanje nedostataka.

(6) Finansijski subjekt je, i nakon dobijanja potvrde o sprovedenom testiranju, odgovoran za uticaj objedinjenog TLPT-a iz člana 30 stav 2 ovog zakona.

Zahtjevi za lica koja su angažovana za sprovođenje TLPT-a

Član 32

(1) Finansijski subjekt je dužan da za potrebe sprovođenja TLPT-a iz člana 29 ovog zakona angažuje interna ili eksterna lica.

(2) Finansijski subjekt koji za potrebe sprovođenja TLPT-a angažuje interna lica, dužan je da za svako treće sprovođenje TLPT-a angažuje eksterna lica.

(3) Angažovana lica za potrebe sprovođenja TLPT-a iz stava 1 ovog člana moraju da:

- 1) ispunjavaju najviše standarde primjerenosti i ugleda;
- 2) posjeduju tehničke i organizacione sposobnosti i posebno stručno znanje u oblasti saznanja o prijetnjama, penetracionih testiranja i testiranja crvenog tima;
- 3) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju u skladu sa zakonom kojim se uređuje postupak akreditacije, ili se pridržavaju formalnih kodeksa ponašanja ili etičkih okvira;
- 4) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju druge države članice;
- 5) dostave nezavisno uvjerenje ili revizorski izvještaj kojim se potvrđuje da dobro upravljaju rizicima povezanim sa sprovođenjem TLPT-a, što uključuje adekvatnu zaštitu povjerljivih informacija finansijskog subjekta i mehanizme pravne zaštite u pogledu poslovnih rizika finansijskog subjekta;
- 6) koja su propisno i u cjelosti osigurana od profesionalne odgovornosti, uključujući i rizike od protivpravnog i nemarnog postupanja.

(4) U slučaju angažovanja internih lica za sprovođenje TLPT-a, finansijski subjekt dužan je da obezbijedi da su, pored zahtjeva iz stava 3 ovog člana, ispunjeni i sljedeći zahtjevi:

- 1) to angažovanje je odobrio nadležni organ, odnosno nadležni organ kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona;
- 2) nadležni organ je potvrdio da je finansijski subjekt obezbijedio dovoljne resurse i preduzeo mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja testiranja; i
- 3) pružalac saznanja o prijetnjama nije dio finansijskog subjekta.

(5) Finansijski subjekt je dužan da obezbijedi da se ugovorom zaključenim sa eksternim licem koje sprovodi TLPT obezbjeđuje dobro upravljanje rezultatima TLPT-a i da bilo kakva obrada podataka u vezi sa tim, uključujući generisanje, izradu, agregiranje,

skladištenje, izvještavanje, saopštavanje i uništavanje podataka, ne stvara rizike za tog finansijskog subjekta.

V. UPRAVLJANJE IKT RIZIKOM POVEZANIM SA TREĆIM STRANAMA

Ključna načela dobrog upravljanja IKT rizikom povezanim sa trećim stranama

Član 33

(1) Finansijski subjekt je dužan da upravlja IKT rizikom povezanim sa trećim stranama kao sastavnim dijelom IKT rizika, u okviru sistema upravljanja IKT rizicima iz člana 10 ovog zakona, u skladu sa sljedećim principima:

- 1) finansijski subjekt koji je zaključio ugovor o korišćenju IKT usluga radi obavljanja svojih poslovnih aktivnosti, u svakom trenutku snosi punu odgovornost za usklađenost sa ovim zakonom i propisima kojima se uređuje poslovanje tog finansijskog subjekta;
- 2) finansijski subjekt upravlja IKT rizikom povezanim sa trećim stranama u skladu sa principom proporcionalnosti, uzimajući u obzir:
 - prirodu, obim, složenost i značaj zavisnosti u oblasti IKT-a;
 - rizike koji proizilaze iz ugovora o korišćenju IKT usluga zaključenih sa trećim stranama koje pružaju IKT usluge, uzimajući u obzir kritičnost ili značaj konkretne usluge, procesa ili funkcije i potencijalni uticaj na kontinuitet i dostupnost finansijskih usluga i aktivnosti, na pojedinačnom nivou i na nivou grupe.

(2) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt i nije subjekt iz člana 21 stav 1 ovog zakona, dužan je da usvoji i redovno preispituje strategiju upravljanja IKT rizikom povezanim sa trećim stranama, uzimajući u obzir strategiju IKT nabavke od više dobavljača iz člana 12 stav 3 ovog zakona, kada je to primjenljivo.

(3) Strategija iz stava 2 ovog člana obuhvata politiku korišćenja IKT usluga koje pružaju treće strane za podršku kritičnih ili važnih funkcija finansijskog subjekta, i primjenjuje se na pojedinačnoj i, kada je to primjenljivo, na potkonsolidovanoj i konsolidovanoj osnovi.

(4) Organ upravljanja finansijskog subjekta dužan je da, na osnovu procjene ukupnog rizičnog profila finansijskog subjekta, obima i složenosti poslovnih usluga, redovno preispituje rizike identifikovane u vezi sa ugovorima o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije.

(5) Prije zaključenja ugovora o korišćenju IKT usluga, finansijski subjekt je dužan da:

- 1) procijeni da li se ugovorom predviđa korišćenje IKT usluga koje podržavaju kritične ili važne funkcije;
- 2) provjeri da li su ispunjeni zahtjevi nadležnog organa za zaključenje ugovora;
- 3) identifikuje i procijeni sve relevantne rizike povezane sa ugovorom, uključujući i mogućnost da ugovor doprinese povećanju rizika IKT koncentracije iz člana 37 ovog zakona;
- 4) sprovede detaljnu analizu potencijalnih trećih strana koje pružaju IKT usluge i, kroz postupak odabira i procjene, obezbijedi da je odabrana treća strana adekvatna za pružanje tih usluga;

- 5) identifikuje i procijeni sukobe interesa koje bi taj ugovor mogao da izazove.

Registar informacija o ugovorima o korišćenju IKT uslugama i obavještanje nadležnog organa

Član 34

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na pojedinačnoj, kao i na potkonsolidovanoj i konsolidovanoj osnovi, vodi i ažurira registar informacija o svim ugovorima o korišćenju IKT usluga koje pružaju treće strane.

(2) Informacije o ugovorima iz stava 1 ovog člana moraju biti evidentirane tako da se ugovori koji se odnose na IKT usluge za podršku kritičnih ili važnih funkcija razlikuju od ugovora koji se ne odnose na te funkcije.

(3) Finansijski subjekt je dužan da najmanje jednom godišnje dostavi nadležnom organu izvještaj o broju novih ugovora o korišćenju IKT usluga, kategorijama trećih strana koje pružaju IKT usluge, vrsti ugovora i IKT uslugama i funkcijama koje se pružaju.

(4) Finansijski subjekt je dužan da nadležnom organu, na njegov zahtjev, stavi na raspolaganje pojedine djelove ili cjelokupan registar informacija iz stava 1 ovog člana, uključujući i druge informacije koje su nadležnom organu potrebne za sprovođenje nadzora.

(5) Finansijski subjekt je dužan da blagovremeno obavijesti nadležni organ o svakom planiranom ugovoru u skladu sa kojim namjerava da koristi IKT usluge za podršku kritičnih ili važnih funkcija, kao i o svakoj funkciji koja je podržana ugovorom o korišćenju IKT usluga, a koja postane kritična ili važna funkcija.

Standardi bezbjednosti i revizije treće strane koja pruža IKT usluge

Član 35

(1) Finansijski subjekt može da zaključi ugovor sa trećom stranom koja pruža IKT usluge, ukoliko ta treća strana primjenjuje odgovarajuće standarde informacione bezbjednosti.

(2) U slučaju kada se ugovor iz stava 1 ovog člana odnosi na usluge kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da, prije zaključenja tog ugovora, utvrdi da treća strana koja pruža IKT usluge primjenjuje najnovije i najviše standarde informacione bezbjednosti.

(3) Radi ostvarivanja prava pristupa, sprovođenja provjera i revizija nad trećom stranom koja pruža IKT usluge, finansijski subjekt dužan je da, primjenom pristupa zasnovanog na procjeni rizika, unaprijed odredi učestalost provjera i revizija, kao i oblasti u kojima će se sprovesti, u skladu sa opšteprihvaćenim revizorskim standardima i, kada je to primjenljivo, zahtjevima nadležnog organa u pogledu primjene tih standarda.

(4) U slučaju da ugovor zaključen sa trećom stranom koja pruža IKT usluge iz stava 1 ovog člana obuhvata korišćenje IKT usluga koje podrazumijevaju visok stepen tehničke složenosti, finansijski subjekt je dužan da provjeri da li revizori, bilo da su interni, eksterni ili grupa revizora, posjeduju odgovarajuće vještine i znanja neophodna za efikasno sprovođenje relevantnih revizija i procjena.

Raskid ugovora i izlazne strategije

Član 36

(1) Finansijski subjekt je dužan da obezbijedi da se ugovor o korišćenju IKT usluga može raskinuti u sljedećim slučajevima:

- 1) treća strana koja pruža IKT uslugu značajno je prekršila zakon, propis ili ugovorne obaveze;
- 2) praćenjem IKT rizika povezanog sa trećom stranom utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjene u izvršavanju funkcija koje se pružaju na osnovu ugovora, uključujući bitne promjene koje utiču na ugovorni odnos ili stanje treće strane koja pruža IKT usluge;
- 3) treća strana koja pruža IKT usluge je pokazala slabosti u pogledu upravljanja ukupnim IKT rizikom, a naročito u načinu na koji obezbjeđuje dostupnost, autentičnost, integritet i povjerljivost podataka, bez obzira da se radi o podacima o ličnosti, osjetljivim ili drugim podacima;
- 4) nadležni organ više nije u mogućnosti da sprovodi efikasan nadzor finansijskog subjekta zbog uslova ili okolnosti koje se tiču ugovornog odnosa.

(2) Finansijski subjekt je dužan da utvrdi izlazne strategije za IKT usluge koje podržavaju kritične ili važne funkcije.

(3) Izlaznim strategijama iz stava 2 ovog člana moraju se uzeti u obzir rizici koji mogu nastati na nivou trećih strana koje pružaju IKT usluge, a naročito mogućnost propasti tih trećih strana, pogoršanje kvaliteta IKT usluga koje se pružaju, poremećaji u poslovanju usljed neadekvatnog ili neuspješnog pružanja IKT usluga, bilo koji značajan rizik koji se odnosi na adekvatnost i kontinuitet pružanja konkretne usluge, kao i mogućnost raskida ugovora sa trećom stranom koja pruža IKT usluge u slučaju iz stava 1 ovog člana.

(4) Finansijski subjekt je dužan da obezbijedi da raskid ugovora o korišćenju IKT usluga ne dovede do:

- 1) poremećaja poslovnih aktivnosti tog finansijskog subjekta;
- 2) ograničavanja usklađenosti sa regulatornim zahtjevima;
- 3) narušavanja kontinuiteta i kvaliteta usluga koje se pružaju klijentima.

(5) Finansijski subjekt je dužan da obezbijedi da su planovi za raskid ugovornih odnosa iz stava 1 ovog člana sveobuhvatni, dokumentovani i da se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, dovoljno testiraju i periodično preispituju.

(6) Finansijski subjekt je dužan da utvrdi alternativna rješenja i razvije tranzicione planove koji mu omogućavaju da, na siguran i cjelovit način, prenese ugovorene IKT usluge i povezane podatke sa treće strane koja pruža IKT usluge na alternativne pružaoce usluga ili ih reintegriše u okviru sopstvenih kapaciteta, kao i da obezbijedi njihovo uklanjanje kod treće strane koja je pružala IKT usluge.

(7) Finansijski subjekt je dužan da uspostavi odgovarajuće mjere za nepredviđene situacije radi očuvanja kontinuiteta poslovanja u slučaju nastanka okolnosti iz stava 3 ovog člana.

Procjena rizika IKT koncentracije na nivou finansijskog subjekta

Član 37

(1) Prilikom identifikacije i procjene rizika iz člana 33 stav 5 tačka 3 ovog zakona, finansijski subjekt je dužan da uzme u obzir da li bi zaključivanje ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije dovelo do:

- 1) angažovanja treće strane koja pruža IKT uslugu koja se ne može lako zamijeniti; ili
 - 2) postojanja više ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije sa istom trećom stranom koja pruža IKT usluge ili sa usko povezanim trećim stranama koje pružaju IKT usluge.
- (2) Finansijski subjekt je dužan da procijeni prednosti i troškove alternativnih rješenja, kao što je angažman različitih trećih strana koje pružaju IKT usluge, uzimajući u obzir da li i na koji način predviđena rješenja odgovaraju poslovnim potrebama i ciljevima utvrđenim u strategiji digitalne operativne otpornosti tog finansijskog subjekta.
- (3) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđeno da treća strana koja pruža IKT uslugu, radi pružanja tih usluga, može kao podizvođače angažovati druge pružaoce IKT usluga, finansijski subjekt je dužan da procijeni prednosti i rizike koji mogu proizaći iz tog angažovanja, naročito u slučaju angažovanja IKT podizvođača sa sjedištem u trećoj zemlji.
- (4) U slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da razmotri propise koji bi se primjenjivali u slučaju insolventnosti treće strane koja pruža IKT usluge, uključujući stečaj i likvidaciju, kao i sva ograničenja koja bi mogla nastati u slučaju potrebe za hitnim povratkom podataka finansijskog subjekta.
- (5) U slučaju da se ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije zaključuje sa trećom stranom koja pruža IKT usluge sa sjedištem u trećoj zemlji, finansijski subjekt je dužan da, pored elemenata iz stava 4 ovog člana, razmotri i usklađenost sa odredbama propisa kojima se uređuje zaštita podataka, kao i mogućnost sprovođenja zakona u toj trećoj zemlji.
- (6) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđena mogućnost angažovanja podizvođača, finansijski subjekt je dužan da procijeni da li, i na koji način, potencijalno dugi ili složeni lanci podugovaranja mogu uticati na njegovu sposobnost da u potpunosti prati ugovorene funkcije, kao i na mogućnost nadležnog organa da sprovodi efikasan nadzor tog finansijskog subjekta.

Ključne ugovorne odredbe

Član 38

- (1) Prava i obaveze finansijskog subjekta i treće strane koja pruža IKT usluge moraju biti uređene ugovorom.
- (2) Ugovor iz stava 1 ovog člana sadrži i sporazume o nivou usluga, i mora biti dostupan ugovornim stranama u papirnom ili elektronskom obliku koji se može preuzeti u pristupačnom i trajnom formatu.
- (3) Ugovor o korišćenju IKT usluga mora da sadrži:
 - 1) jasan i potpun opis svih funkcija i IKT usluga koje će pružati treća strana koja pruža IKT usluge;
 - 2) odredbe da li treća strana koja pruža IKT usluge može angažovati podizvođače radi pružanja IKT usluge kojom se podržava kritična ili važna funkcija, ili radi pružanja njenih bitnih djelova, i pod kojim uslovima;

- 3) lokacije, odnosno regije ili države, sa kojih će se pružati ugovorene i, kada je to primjenljivo, podugovorene funkcije i IKT usluge, kao i lokacije na kojima će se obrađivati podaci, uključujući lokacije na kojima će se skladištiti podaci;
 - 4) obavezu treće strane koja pruža IKT usluge da unaprijed obavijesti finansijski subjekt o namjeri promjene lokacija iz tačke 3 ovog stava;
 - 5) odredbe o zaštiti dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, uključujući podatke o ličnosti;
 - 6) odredbe kojima se finansijskom subjektu obezbjeđuje mogućnost pristupa, obnove i povratka podataka o ličnosti i drugih podataka u slučaju insolventnosti, sanacije ili prestanka poslovanja treće strane koja pruža IKT usluge, kao i u slučaju raskida ugovora;
 - 7) opise nivoa usluga, uključujući njihova ažuriranja, odnosno izmjene;
 - 8) obavezu treće strane koja pruža IKT usluge da pruži pomoć finansijskom subjektu bez dodatne naknade ili po unaprijed utvrđenoj cijeni, u slučaju IKT incidenta koji je povezan sa IKT uslugom koju ta treća strana pruža finansijskom subjektu;
 - 9) obavezu treće strane koja pruža IKT usluge da u sarađuje sa nadležnim organom i organom koji je zadužen za sanaciju finansijskog subjekta u skladu sa zakonom kojim se uređuje sanacija finansijskog subjekta, uključujući i saradnju sa licima koja ovlaste ti organi;
 - 10) prava i uslove za raskid ugovora, sa rokovima za dostavljanje obavještenja o namjeri raskida ugovora, u skladu sa zahtjevima organa iz tačke 9 ovog stava;
 - 11) uslove za učešće treće strane koja pruža IKT usluge u programima za podizanje svijesti o IKT bezbjednosti i obukama o digitalnoj operativnoj otpornosti u skladu sa odredbama člana 19 stav 12 ovog zakona.
- (4) Ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije mora, pored elemenata iz stava 3 ovog člana, da sadrži i:
- 1) detaljan opis nivoa usluga, uključujući njihova ažuriranja i izmjene, sa preciznim kvantitativnim i kvalitativnim ciljevima učinka u okviru dogovorenih nivoa usluga, kako bi se finansijskom subjektu omogućilo efikasno praćenje IKT usluga i preduzimanje, bez odlaganja, odgovarajućih korektivnih mjera u slučaju da dogovoreni nivoi usluga nisu ispunjeni;
 - 2) obavezu treće strane koja pruža IKT usluge da finansijskom subjektu dostavlja obavještenja i izvještaje, sa rokovima za njihovo dostavljanje, uključujući i obavještenja o svim okolnostima koje bitno utiču ili bi mogle bitno uticati na sposobnost treće strane koja pruža IKT usluge da efikasno pruža IKT usluge kojima se podržavaju kritične ili važne funkcije, u skladu sa dogovorenim nivoima usluga;
 - 3) zahtjeve koje treća strana koja pruža IKT usluge mora ispunjavati u pogledu primjene i testiranja planova za nepredviđene okolnosti, kao i primjene IKT bezbjednosnih mjera, alata i politika kojima se obezbjeđuje adekvatan nivo bezbjednosti, potreban finansijskom subjektu za pružanje usluga u skladu sa zakonom;
 - 4) obavezu treće strane koja pruža IKT usluge da učestvuje u TLPT-u finansijskog subjekta i bude maksimalno kooperativna tokom njegovog sprovođenja, u skladu sa odredbama čl. 29 do 32 ovog zakona;

5) pravo kontinuiranog praćenja učinka treće strane koja pruža IKT usluge, što obuhvata:

- neograničena prava finansijskog subjekta, treće strane koju je ovlastio finansijski subjekt i nadležnog organa na pristup, sprovođenje provjera, reviziju, odnosno nadzor nad i kod treće strane koja pruža IKT usluge, kao i pravo na dobijanje kopija relevantne dokumentacije treće strane koja pruža IKT usluge, tako da se ostvarivanje tih prava ne može isključiti ili ograničiti drugim ugovorima ili politikama;
- pravo da se, u slučaju kada bi ostvarivanje prava iz alineje 1 ove tačke moglo ugroziti prava drugih klijenata treće strane koja pruža IKT usluge, dogovore alternativni načini provjere učinka treće strane koja pruža IKT usluge, kojima se obezbjeđuje razuman nivo uvjerenja o kvalitetu i bezbjednosti pruženih usluga;
- obavezu treće strane koja pruža IKT usluge da u potpunosti sarađuje tokom neposrednih provjera, revizija i nadzora koje sprovodi nadležni organ, finansijski subjekt ili treća strana koju je ovlastio finansijski subjekt;
- obavezu treće strane koja pruža IKT usluge da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, tokom nadzora koji sprovodi taj organ;
- obavezu dostavljanja informacija potrebnih za određivanje obima, procedura koje će se primjenjivati i učestalosti provjera, revizija i nadzora iz al. 3 i 4 ove tačke.

6) odredbe neophodne za realizaciju izlazne strategije, naročito obavezni i adekvatni tranzicioni period:

- tokom kojeg će treća strana koja pruža IKT usluge nastaviti pružanje relevantnih funkcija i IKT usluga, radi ublažavanja rizika od nastanka poremećaja kod finansijskog subjekta ili radi obezbjeđivanja njegove efikasne sanacije i restrukturiranja;
- tokom kojeg finansijski subjekt može zamijeniti treću stranu koja pruža IKT usluge ili reintegrirati IKT usluge u okviru sopstvenih kapaciteta, u skladu sa složenošću tih usluga.

(5) Izuzetno od stava 4 tačka 5 ovog člana, finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt može ugovoriti sa trećom stranom koja pruža IKT usluge da se pravo tog finansijskog subjekta na pristup, sprovođenje provjera i reviziju nad i kod treće strane koja pruža IKT usluge može povjeriti nezavisnoj trećoj strani, koju odredi treća strana koja pruža IKT usluge, u kom slučaju finansijski subjekt od nezavisne treće strane, u svakom trenutku, može zahtijevati informacije i potvrde o učinku treće strane koja pruža IKT usluge.

(6) Prilikom usaglašavanja odredbi ugovora sa trećom stranom koja pruža IKT usluge, finansijski subjekt je dužan da razmotri primjenu standardizovanih ugovornih klauzula koje su javni organi razvili za određene usluge.

VI. RAZMJENA INFORMACIJA

Razmjena informacija i saznanja o sajber prijetnjama

Član 39

(1) Finansijski subjekti mogu međusobno razmjenjivati informacije i saznanja o sajber prijetnjama, uključujući indikatore ugroženosti, taktike, tehnike i procedure, bezbjednosna upozorenja i alate za konfiguraciju, u mjeri u kojoj ta razmjena:

- 1) ima za cilj jačanje digitalne operativne otpornosti finansijskih subjekata, naročito podizanjem svijesti o sajber prijetnjama, ograničavanje ili sprečavanje njihovog širenja, unapređenje odbrambenih kapaciteta, tehnika za otkrivanje prijetnji, strategija za ublažavanje uticaja ili postupaka odgovora i oporavka;
- 2) se sprovodi u okviru pouzdane zajednice finansijskih subjekata;
- 3) se ostvaruje kroz sporazume za razmjenu informacija kojima se štiti potencijalno osjetljiva priroda tih informacija, koji su uređeni pravilima ponašanja kojima se obezbjeđuje potpuna zaštita povjerljivih poslovnih informacija, podataka o ličnosti u skladu sa propisom kojim se uređuje zaštita podataka o ličnosti i primjena pravila u oblasti zaštite konkurencije.

(2) Sporazumima za razmjenu informacija iz stava 1 tačka 3 ovog člana moraju se utvrditi uslovi za učešće u razmjeni informacija i, kada je to primjenjivo, učešće i uloga javnih organa koji mogu biti uključeni u tim sporazumima, trećih strana koje pružaju IKT usluge, kao i operativni elementi, uključujući i upotrebu posebnih IT platformi.

(3) Finansijski subjekt je dužan da obavijesti nadležni organ bez odlaganja ako je učesnik u sporazumu za razmjenu informacija iz stava 1 tačka 3 ovog člana, odnosno kada prestane sa učešćem u tom sporazumu.

VII. NADZOR NAD SPROVOĐENJEM ODREDBI OVOG ZAKONA I NADZORNE MJERE

Obim nadležnosti

Član 40

(1) Nadzor nad sprovođenjem ovog zakona vrši nadležni organ.

(2) U sprovođenju nadzora iz stava 1 ovog člana, nadzorni organ:

- 1) izriče mjere finansijskom subjektu;
- 2) podnosi predloge za pokretanje prekršajnih postupaka zbog kršenja odredbi ovog zakona.

(3) Nadzor iz stava 2 tačka 1 ovog člana sprovodi se u skladu sa ovim zakonom i zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta.

(4) U vršenju nadzora iz stava 1 ovog člana, nadležni organ može naročito da:

- 1) pristupi svim dokumentima ili podacima u bilo kom obliku koje smatra relevantnim za izvršavanje svojih ovlašćenja i pribavi kopije tih dokumenata ili podataka;
- 2) sprovede neposredni nadzor ili kontrolu, koji uključuju, ali nisu ograničeni na:
 - ovlašćenje da od finansijskog subjekta i lica zaposlenih u finansijskom subjektu zahtijeva pisana i usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole;
 - obavljanje razgovora sa bilo kojim fizičkim ili pravnim licem za koje ocijeni da ima relevantna saznanja, uz izričitu saglasnost tog lica, u svrhu prikupljanja informacija koje se odnose na predmet kontrole;
- 3) zahtijeva sprovođenje korektivnih mjera zbog kršenja odredbi ovog zakona.

(5) Pored mjera koje je nadležni organ ovlašten da izriče u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, nadležni organ je ovlašten da u vršenju nadzora u skladu sa ovim zakonom:

- 1) naloži finansijskom subjektu i odgovornom licu u finansijskom subjektu da prekine, postupanje koje predstavlja kršenje ovog zakona i propisa donesenih na osnovu ovog zakona;
- 2) naloži finansijskom subjektu da privremeno ili trajno prekine sa postupanjem koje nadležni organ smatra kršenjem ovog zakona i propisa donesenih na osnovu ovog zakona i da spriječi ponavljanje takvog postupanja;
- 3) izrekne kaznu, uključujući i novčanu kaznu, kako bi se obezbijedilo da finansijski subjekt nastavi sa ispunjavanjem zahtjeva iz ovog zakona i propisa donesenih na osnovu ovog zakona;
- 4) uputi zahtjev, u skladu sa zakonom, za dostavljanje evidencije telekomunikacionog operatera o prometu podataka koji su od značaja za utvrđivanje povrede ovog zakona i propisa donesenih na osnovu ovog zakona, kada postoji opravdana sumnja na takvu povredu;
- 5) izda javno obavještenje o kršenju zakona, u kojem može da navede identitet finansijskog subjekta koji je bio predmet nadzora, odnosno kontrole, lica u tom finansijskom subjektu odgovorna za kršenje zakona i propisa donesenih na osnovu ovog zakona kao i prirodu tog kršenja.

(6) Nadležni organ može naložiti finansijskom subjektu da razriješi člana upravnog odbora ili drugo lice sa rukovodeće funkcije u tom finansijskom subjektu kada utvrdi njegovu odgovornost za kršenje ovog zakona.

(7) Finansijski subjekt kome je naložena mjera iz st. 5 ili 6 ovog člana, dužan je da izvrši tu mjeru na način i u roku utvrđenim rješenjem o izricanju mjere.

(8) Finansijski subjekt dužan je da u potpunosti sarađuje sa nadležnim organom tokom postupka nadzora ili kontrole i da na zahtjev nadležnog organa za potrebe sprovođenja nadzora ili kontrole dostavi zahtijevana pisana ili usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole.

Način utvrđivanja mjera

Član 41

(1) Nadležni organ izvršava ovlaštenje za izricanje mjera iz člana 40 ovog zakona, u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, i to:

- 1) neposrednim postupanjem;
- 2) u saradnji sa nadležnim i drugim organima;
- 3) povjeravanjem pojedinih poslova drugim organima, u okviru sopstvene odgovornosti; ili
- 4) podnošenjem zahtjeva nadležnom pravosudnom organu.

(2) Prilikom odlučivanja o vrsti i visini mjere iz člana 40 stav 4 ovog zakona, nadležni organ uzima u obzir stepen namjere ili nehat u postupanju kojim je izvršeno kršenje odredbi ovog zakona i propisa donesenih na osnovu ovog zakona kao i sve druge relevantne okolnosti, naročito:

- 1) značaj, težinu i trajanje kršenja, odnosno ponavljanje ili učestalost kršenja;
- 2) stepen odgovornosti finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje;

- 3) finansijsku sposobnost finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje;
- 4) iznos stečene dobiti ili izbjegnutog gubitka finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, ako se taj iznos može utvrditi;
- 5) gubitke trećih lica nastale kršenjem, ako se mogu utvrditi;
- 6) saradnju finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, sa nadležnim organom, bez prejudiciranja obaveze povraćaja koristi ili izbjegnutog gubitka;
- 7) prethodna kršenja i izrečene mjere finansijskom subjektu, odnosno fizičkom licu odgovornom za kršenje.

(3) Mjere nadležnog organa izrečene u skladu sa odredbama ovog zakona, moraju biti efikasne, srazmjerne i odvraćajuće.

Saradnja u slučaju krivičnog djela

Član 42

Nadležni organ je dužan da u okviru svoje nadležnosti sarađuje sa pravosudnim organima i organima nadležnim za sprovođenje krivičnih sankcija radi razmjene informacija potrebnih za vođenje istraga i postupka u vezi sa sprovođenjem sankcija za krivično djelo u oblasti digitalne operativne otpornosti propisano zakonom.

Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima

Član 43

(1) Nadležni organ na svojoj internet stranici, bez odlaganja, objavljuje podatke o novčanim kaznama izrečenim pravosnažnim rješenjem iz člana 40 stav 4 tačka 3 ovog zakona i pravosnažnim kaznama finansijskom subjektu i odgovornom licu u finansijskom subjektu izrečenim u prekršajnom postupku zbog kršenja odredbi ovog zakona ili propisa donesenih na osnovu ovog zakona.

(2) Podaci iz stava 1 ovog člana sadrže informacije o vrsti i prirodi kršenja, naziv finansijskog subjekta i ime i prezime odgovornih lica u finansijskom subjektu kome je izrečena kazna.

(3) Izuzetno od st. 1 i 2 ovog člana, ako na pojedinačnoj osnovi nadležni organ procijeni da objavljivanje identiteta finansijskog subjekta ili ličnih podataka odgovornih lica u finansijskom subjektu nije srazmjerno utvrđenom kršenju, ili bi objavljivanje ugrozilo stabilnost finansijskog tržišta, istražne radnje u krivičnom postupku koje su u toku, ili bi objavljivanje prouzrokovalo nesrazmjernu štetu za finansijski subjekt ili odgovorna lica, koju je moguće utvrditi, nadležni organ može da:

- 1) odloži objavljivanje podataka iz st. 1 i 2 ovog člana do prestanka razloga za neobjavljivanje;
- 2) izvrši objavljivanje na način kojim se ne odaju podaci iz st. 1 i 2 ovog člana, s tim što se i to objavljivanje može odložiti;
- 3) ne objavi podatke iz st. 1 i 2 ovog člana ako ocijeni da opcije iz tač. 1 i 2 ovog stava ne mogu u dovoljnoj mjeri obezbijediti stabilnost finansijskog tržišta ili da to objavljivanje nije srazmjerno težini izrečene kazne.

(4) Podaci iz st. 1, 2 i 3 ovog člana ostaju na internet stranici nadležnog organa pet godina od dana objavljivanja.

VIII. SARADNJA NADLEŽNIH ORGANA SA DRUGIM ORGANIMA

Saradnja sa organima iz zakona kojim se uređuje informaciona bezbjednost

Član 44

(1) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost određen kao jedinstvena nacionalna kontakt tačka za informacionu bezbjednost.

(2) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost nadležan za zaštitu finansijskih subjekata od sajber prijetnji i incidenata i od njega može zatražiti relevantnu pomoć.

(3) Saradnja iz stava 2 ovog člana uređuje se sporazumima između nadležnih organa i tog organa.

Saradnja sa organima Evropske unije i organima trećih država

Član 45

(1) Nadležni organ može, u cilju jačanja saradnje u oblasti upravljanja IKT rizicima koji se odnose na angažovanje trećih strana, zaključivati sporazume sa nadzornim i regulatornim organima Evropske unije i trećih država.

(2) Sporazumi iz stava 1 ovog člana mogu obuhvatati razmjenu iskustava i primjera dobre prakse, saradnju u preispitivanju okvira upravljanja IKT rizicima, mjera za njihovo ublažavanje, kao i razmjenu informacija u vezi sa postupanjem u slučaju IKT incidenata.

(3) Nadležni organi dužni su da sarađuju sa EBA-om, ESMA-om i EIOPA-om u sprovođenju aktivnosti nadzora kritičnih trećih strana koje pružaju IKT usluge radi razmjene podataka, informacija o incidentima, mjerama i rizicima, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.

(4) Nadležni organ je dužan da obavještava EBA-u, ESMA-u i EIOPA-u o objedinjenim podacima o zavisnostima finansijskih subjekata u Crnoj Gori od kritičnih trećih strana koje pružaju IKT usluge, radi usklađivanja sa praksom na nivou Evropske unije i učešća u zajedničkim mehanizmima nadzora.

(5) Podaci iz stava 4 ovog člana prikupljaju se i dostavljaju iz registara ugovora koje finansijski subjekat vodi u skladu sa ovim zakonom.

(6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlašćenja glavnog nadzornog organa u pogledu sprovođenja nadzora.

(7) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om i EIOPA-om i drugim relevantnim organima, u vezi sa učešćem u uspostavljanju mehanizma za razmjenu dobre prakse u cilju unapređenja međusektorske svijesti o stanju i identifikaciji zajedničkih ranjivosti i rizika u oblasti sajber bezbjednosti, uključujući i učešće u razvoju i

sprovođenju vježbi za upravljanje kriznim i nepredviđenim situacijama, scenarijima sajber napada i drugih aktivnosti koje doprinose uspostavljanju efikasnog i koordinisanog odgovora na nivou Evropske unije u slučaju značajnih prekograničnih IKT incidenata ili srodnih prijetnji sa sistemskim uticajem na finansijski sektor, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.

(8) Nadležni organ je dužan da obavještava Evropsku komisiju EBA-u, ESMA-u i EIOPA-u o:

- 1) propisima kojima se bliže uređuju zahtjevi iz ovog zakona, kao i o izmjenama tih propisa u rokovima propisanim Regulativom (EU) 2022/2554;
- 2) informacijama koje se razmjenjuju sa pravosudnim organima i organima nadležnim za sprovođenje krivičnih sankcija u skladu sa članom 42 ovog zakona.

IX. POSLOVNA TAJNA I ZAŠTITA PODATAKA O LIČNOSTI

Čuvanje poslovne tajne

Član 46

(1) Sve povjerljive informacije koje nadležni organ primi, razmijeni ili prenese u vezi sa sprovođenjem ovog zakona smatraju se tajnom u skladu sa zakonom i podliježu obavezi čuvanja tajne.

(2) Obaveza čuvanja poslovne tajne iz stava 1 ovog člana odnosi se na sva lica zaposlena ili angažovana od strane nadležnog organa, kao i sva druga pravna ili fizička lica kojima nadležni organ, u skladu sa zakonom, povjeri obavljanje pojedinih poslova ili ovlašćenja, uključujući revizore i spoljne eksperte.

(3) Informacije koje predstavljaju poslovnu tajnu ne mogu se saopštavati trećim licima, osim ako je to propisano ovim zakonom ili drugim propisom.

(4) Sve informacije koje se razmjenjuju između nadležnih organa u skladu sa ovim zakonom, a koje se odnose na poslovanje finansijskog subjekta ili operativne uslove, ekonomske ili lične, smatraju se povjerljivim, osim ako nadležni organ prilikom dostavljanja informacija izričito ne navede da se iste mogu objavljivati ili ako je njihovo objavljivanje nužno za vođenje sudskog postupka.

(5) Obavješćavanje i razmjena podataka između nadležnih organa, odnosno između nadležnih organa i drugih organa u skladu sa ovim zakonom, ne predstavlja kršenje obaveze čuvanja povjerljivih informacija utvrđene posebnim zakonom.

Obrada i zaštita podataka o ličnosti

Član 47

(1) Nadležni organ obrađuje podatke o ličnosti samo u mjeri u kojoj je to neophodno za izvršavanje ovlašćenja u skladu sa ovim zakonom, naročito prilikom vršenja nadzora i kontrole, zahtijeva za dostavljanje informacija, komunikacije, objavljivanja informacija, evaluacije, provjere, procjene i izrade planova nadzora.

(2) Obrada podataka o ličnosti iz stava 1 ovog člana vrši se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

(3) Podaci o ličnosti iz stava 1 ovog člana mogu se čuvati samo onoliko koliko je potrebno za vršenje ovlašćenja u vezi sa nadzorom finansijskog subjekta, a najduže 15 godina.

(4) Izuzetno od stava 3 ovog člana, podaci o ličnosti se mogu čuvati duže u slučaju vođenja sudskih postupaka, odnosno do okončanja postupka.

X. PROPISI O DIGITALNOJ OPERATIVNOJ OTPORNOSTI

Propisi Centralne banke o digitalnoj operativnoj otpornosti

Član 48

(1) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje:

- 1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;
- 2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;
- 3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;
- 4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;
- 5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;
- 6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;
- 7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Centralna banka bliže propisuje:

- 1) za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona:
 - kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;
 - kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;
- 2) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje:

- 1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;
- 2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;
- 3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;
- 4) obrasce i postupke za obavješćavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje:

- 1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovode TLPT;
- 2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;
- 3) zahtjeve koji se odnose na:
 - obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;
 - metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;
 - rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona dužan je da postupi u skladu sa propisima Centralne banke iz st. 1 do 8 ovog člana.

Propisi Komisije o digitalnoj operativnoj otpornosti

Član 49

(1) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje:

- 1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;
- 2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;
- 3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;
- 4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;
- 5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;
- 6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;
- 7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Komisija bliže propisuje:

3) za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona:

- kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;
- kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;

4) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje:

- 1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;
- 2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;
- 3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;
- 4) obrasce i postupke za obavješćavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje:

- 1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovedu TLPT;
- 2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;
- 3) zahtjeve koji se odnose na:
 - obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;
 - metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;
 - rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Komisija bliže propisuje kriterijume za pojednostavljeni sistem upravljanja IKT rizicima iz člana 21 ovog zakona.

(10) Finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona dužan je da postupi u skladu sa propisima Komisije iz st. 1 do 9 ovog člana.

Propisi Agencije o digitalnoj operativnoj otpornosti

Član 50

(1) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje:

- 1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;
- 2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;
- 3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;
- 4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;
- 5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;
- 6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;
- 7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Agencija bliže propisuje:

- 1) za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona:
 - kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;
 - kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;
- 2) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje:

- 1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;
- 2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;
- 3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;
- 4) obrasce i postupke za obavješćavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje:

- 1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovedu TLPT;
- 2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;
- 3) zahtjeve koji se odnose na:
 - obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;

- metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;
- rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona dužan je da postupi u skladu sa propisima Agencije iz st. 1 do 8 ovog člana.

Propisi drugih nadležnih organa

Član 51

(1) Propise iz člana 48 ovog zakona za finansijske subjekte iz člana 2 stav 1 tač. 26 i 27 ovog zakona donosi nadležni organ iz člana 3 stav 1 tačka 4 ovog zakona.

(2) Finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona dužan je da postupi u skladu sa propisima iz stava 1 ovog člana.

XI. KAZNENE ODREDBE

Član 52

(1) Novčanom kaznom od 5.000 eura do 40.000 eura kazniće se za prekršaj pravno lice, ako:

- 1) nema uspostavljen sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima u skladu sa članom 10 st. 5 i 6 ovog zakona, radi postizanja visokog nivoa digitalne operativne otpornosti (član 9 stav 2);
- 2) ne odredi organizacioni dio koji je odgovoran za praćenje realizacije ugovora zaključenih sa trećim stranama koje pružaju IKT usluge ili ne imenuje člana višeg rukovodstva koji će biti odgovoran za nadzor povezane izloženosti riziku i pripadajuće dokumentacije (član 9 stav 4);
- 3) nema uspostavljen pouzdan, sveobuhvatan i dobro dokumentovan sistem upravljanja IKT rizicima kao dio opšteg sistema upravljanja rizicima, kojim se omogućava brzo, efikasno i sveobuhvatno tretiranje IKT rizika i obezbjeđuje visok nivo digitalne operativne otpornosti (član 10 st. 1 i 2);
- 4) u skladu sa sistemom upravljanja IKT rizicima ne svede na najmanju moguću mjeru uticaj IKT rizika primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata iz člana 10 stav 2 ovog zakona (član 10 stav 3);

- 5) ne dostavi nadležnom organu, na njegov zahtjev, potpune i ažurne informacije o IKT rizicima i sistemu upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona (član 10 stav 4);
- 6) ne dodijeli odgovornost za upravljanje i nadzor nad IKT rizikom kontrolnoj funkciji ili ne obezbijedi odgovarajući nivo njene nezavisnosti, na način da se izbjegava sukob interesa i razdvajanje poslova u kojima IKT rizik nastaje, poslova kontrolnih funkcija i poslova interne revizije, u skladu sa modelom tri linije odbrane ili internim modelom za upravljanje i kontrolu rizika (član 10 st. 5 i 6);
- 7) kontinuirano ne unaprjeđuje sistem upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona na osnovu iskustava stečenih kroz njegovu praktičnu primjenu i praćenje, i ako taj ne preispituje i ne ažurira na način propisan članom 11 stav 1 ovog zakona (član 11 st. 1 i 2);
- 8) ne dostavi nadležnom organu, na njegov zahtjev, izvještaj o preispitivanju i ažuriranju sistema upravljanja IKT rizicima (član 11 stav 3);
- 9) ne obezbijedi redovne interne revizije sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, u skladu sa planom revizije, od strane nezavisnih revizora koji posjeduju znanje, vještine i iskustvo u oblasti IKT rizika (član 11 st. 4 i 5);
- 10) ne uspostavi formalan proces koji omogućava blagovremeno otklanjanje ključnih nepravilnosti i nedostataka utvrđenih revizijom iz člana 11 stav 4 ovog zakona, kao i adekvatnu primjenu i praćenje tog postupka (član 11 stav 6);
- 11) u strategiji digitalne operativne otpornosti, koja predstavlja sastavni dio sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, ne utvrdi način primjene tog sistema (član 12 st. 1 i 2);
- 12) ne koristi ili ne održava ažurnim IKT sisteme, protokole i alate na način propisan članom 13 ovog zakona (član 13);
- 13) ne identifikuje, ne klasifikuje ili ne dokumentuje adekvatno sve poslovne funkcije podržane IKT-om, zaduženja i odgovornosti, informacionu imovinu i IKT imovinu koja podržava te funkcije ili njihove uloge i međuzavisnosti u pogledu IKT rizika (član 14 stav 1);
- 14) po potrebi, a najmanje jednom godišnje ne preispituje adekvatnost klasifikacije iz člana 14 stav 1 ovog zakona i cjelokupne pripadajuće dokumentacije (član 14 stav 2);
- 15) kontinuirano ne identifikuje sve izvore IKT rizika a naročito izloženosti riziku prema drugim finansijskim subjektima i od drugih finansijskih subjekata, ili ne procjenjuje sajber prijetnje i IKT ranjivosti koje se odnose na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu (član 14 stav 3);
- 16) redovno, a najmanje jednom godišnje, ne razmatra scenarije rizika koji mogu uticati na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu (član 14 stav 4);
- 17) nije sproveo procjenu rizika u slučaju svake značajne promjene u infrastrukturi mrežnih i informacionih sistema i procesima ili procedurama koje utiču na njegove poslovne funkcije podržane IKT-om, informacionu imovinu ili IKT imovinu (član 14 stav 5);
- 18) ne identifikuje svu informacionu imovinu i IKT imovinu, uključujući mrežne resurse, hardversku opremu i imovinu na udaljenim lokacijama, ili ne evidentira posebno informacionu imovinu i IKT imovinu koja se smatra kritičnom (član 14 stav 6);

- 19) ne dokumentuje konfiguraciju informacione imovine i IKT imovine i informacije o povezanosti i međuzavisnosti između različite informacione i IKT imovine (član 14 stav 7);
- 20) ne identifikuje i ne dokumentuje sve procese koji zavise od trećih strana koje pružaju IKT usluge i ako ne identifikuje međusobne povezanosti sa trećim stranama koje pružaju IKT usluge kojima se podržavaju kritične ili važne funkcije (član 14 stav 8);
- 21) radi postupanja u skladu sa članom 14 st. 1, 6, 7 i 8 ovog zakona ne vodi odgovarajuće registre, koje mora da ažurira redovno i u slučaju svake značajne promjene iz člana 14 stav 5 ovog zakona (član 14 stav 9);
- 22) redovno, a najmanje jednom godišnje ne sprovodi procjenu IKT rizika za sve zastarjele IKT sisteme kao i vanredno prije i nakon povezivanja tehnologija, aplikacija ili sistema (član 14 stav 10);
- 23) ne prati kontinuirano ili ne kontroliše bezbjednost i funkcionisanje IKT sistema i alata, i na najmanju moguću mjeru ne svede uticaj IKT rizika na IKT sisteme, primjenom odgovarajućih IKT bezbjednosnih alata, politika i procedura (član 15 stav 1);
- 24) ne osmisli, kreira i/ili nabavi i primijeni politike, procedure, protokole i alate za IKT bezbjednost u cilju obezbjeđivanja otpornosti, kontinuiteta i dostupnosti IKT sistema, a naročito onih koji podržavaju kritične ili važne funkcije, i u cilju održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, bez obzira da li su u stanju mirovanja, upotrebi ili prenosu (član 15 stav 2);
- 25) radi ostvarivanja ciljeva iz člana 15 stav 2 ovog zakona ne koristi IKT rješenja i procese koji su primjereni, u smislu člana 5 ovog zakona, na način propisan članom 15 stav 3 ovog zakona;
- 26) u okviru sistema upravljanja IKT rizicima ne postupa na način propisan članom 15 stav 4 ovog zakona;
- 27) strukturu za upravljanje mrežom i infrastrukturom iz člana 15 stav 4 tačka 2 ovog zakona ne kreira i ne implementira na način kojim se omogućava brzo ukidanje ili segmentiranje mrežnog pristupa, kako bi se u najvećoj mogućoj mjeri ograničilo i spriječilo širenje zaraze, a naročito u slučaju međusobno povezanih finansijskih procesa (član 15 stav 5);
- 28) postupak upravljanja IKT promjenama iz člana 15 stav 4 tačka 5 ovog zakona nije odobren od strane odgovarajućih linija i nivoa odlučivanja finansijskog subjekta, i ne sprovodi se u skladu sa posebno utvrđenim protokolima finansijskog subjekta (član 15 stav 7);
- 29) ne uspostavi mehanizme za brzo otkrivanje neuobičajenih aktivnosti u skladu sa članom 22 ovog zakona, uključujući otkrivanje problema u performansama IKT mreže i IKT incidenata, kao i mehanizme za identifikovanje potencijalnih značajnih jedinstvenih tačaka prekida (član 16 st. 1 i 3);
- 30) ne testira redovno mehanizme za brzo otkrivanje neuobičajenih aktivnosti na način propisan članom 28 ovog zakona (član 16 stav 2);
- 31) ne obezbijedi dovoljne resurse i kapacitete za praćenje aktivnosti korisnika ili otkrivanje neuobičajnih IKT događaja i IKT incidenata, a naročito sajber napada (član 16 stav 4);
- 32) kao pružalac usluga dostave podataka nije uspostavilo sisteme kojima se može efikasno provjeriti da li su izvještaji o trgovanju potpuni i kojima se mogu utvrditi propusti i očigledne greške i zahtijevati ponovni prenos tih izvještaja (član 16 stav 5);

- 33) ne uspostavi, u okviru sistema upravljanja IKT rizicima, na osnovu rezultata postupanja u skladu sa članom 14 ovog zakona, sveobuhvatnu IKT politiku kontinuiteta poslovanja (član 17 st. 1 i 2);
- 34) ne primjenjuje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona pomoću odgovarajućih, namjenskih i dokumentovanih mjera, planova, procedura i mehanizama u cilju ispunjavanja uslova iz člana 17 stav 3 ovog zakona;
- 35) u okviru sistema upravljanja IKT rizicima ne utvrdi i ne primjenjuje odgovarajuće planove za odgovor i oporavak u IKT oblasti (član 17 stav 4);
- 36) ne obezbijedi nezavisnu internu reviziju planova za odgovor i oporavak u IKT oblasti (član 17 stav 5);
- 37) ne uspostavi, ne održava i periodično ne testira odgovarajuće IKT planove kontinuiteta poslovanja, naročito za kritične ili važne funkcije koje, na osnovu zaključenih ugovora, obavljaju ili isporučuju treće strane koje pružaju IKT usluge (član 17 stav 6);
- 38) u okviru opšte politike kontinuiteta poslovanja ne sprovodi analizu uticaja na poslovanje odnosno analizu svoje izloženosti ozbiljnim poremećajima u poslovanju (član 17 stav 7);
- 39) u okviru analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona, na osnovu kvalitativnih i kvantitativnih kriterijuma, korišćenjem raspoloživih internih i eksternih podataka i analize scenarija ne procijeni potencijalni uticaj ozbiljnih poremećaja u poslovanju (član 17 stav 8);
- 40) prilikom vršenja analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona ne uzme u obzir kritičnost identifikovanih poslovnih funkcija, pomoćnih procesa, informacione imovine, zavisnosti od trećih strana, kao i njihovu povezanost i međuzavisnost (član 17 stav 9);
- 41) ne osmisli ili ne koristi IKT imovinu i IKT usluge na način koji je u potpunosti usklađen sa rezultatima analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona, naročito u pogledu obezbjeđivanja adekvatne redundanse svih kritičnih komponenti (član 17 st. 10 i 11);
- 42) ne testira planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planove kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona na način propisan članom 17 stav 12 i 13 ovog zakona ili ne testira planove komunikacije u kriznim situacijama iz člana 20 ovog zakona (član 17 st. 12 i 13);
- 43) redovno ne preispituje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona ili planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona, uzimajući u obzir rezultate testiranja iz člana 17 stav 12 ovog zakona, preporuke revizije i zahtjeve nadležnog organa (član 17 stav 14);
- 44) nije odredilo odgovorno lice ili organizacionu jedinicu za upravljanje kriznim situacijama (član 17 stav 15);
- 45) u slučaju pokretanja IKT planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona ili IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona ne vodi evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna (član 17 stav 16);

- 46) ne dostavi nadležnom organu, na njegov zahtjev, procjenu ukupnih godišnjih troškova i gubitaka koje su prouzrokovali značajni IKT incidenti (član 17 stav 17);
- 47) kao centralno klirinško depozitarno društvo Komisiji ne dostavi kopije rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi (član 17 stav 18);
- 48) u okviru sistema upravljanja IKT rizicima ne razvije ili ne usvoji politike i procedure kojima se na osnovu kritičnosti informacija i povjerljivosti podataka, utvrđuju obim i minimalna učestalost izrade rezervnih kopija podataka, i ne razvije ili ne usvoji procedure i metode za povratak, ponovno uspostavljanje i oporavak (član 18 stav 1);
- 49) ne obezbijedi sisteme za izradu rezervnih kopija podataka koji se mogu koristiti u skladu sa politikama i procedurama za izradu rezervnih kopija podataka iz člana 18 stav 1 tačka 1 ovog zakona, kao i u skladu sa procedurama i metodama za povratak, ponovno uspostavljanje i oporavak iz člana 18 stav 1 tačka 2 ovog zakona (član 18 stav 2);
- 50) korišćenjem sistema za izradu rezervnih kopija podataka iz člana 18 stav 2 ovog zakona ugrozi bezbjednost mrežnih i informacionih sistema ili dostupnost, autentičnost, integritet ili povjerljivost podataka (član 18 stav 3);
- 51) periodično ne testira procedure za izradu rezervnih kopija podataka iz člana 18 stav 1 tačka 1 ovog zakona ili ne testira procedure i metode za povratak, ponovno uspostavljanje i oporavak iz člana 18 stav 1 tačka 2 ovog zakona (član 18 stav 4);
- 52) koristi sopstvene sisteme za povraćaj podataka iz rezervnih kopija, a ne obezbijedi da se za te potrebe koriste IKT sistemi koji su fizički i logički odvojeni od izvornih IKT sistema iz kojih podaci potiču (član 18 stav 5);
- 53) IKT sistemi iz člana 18 stav 5 ovog zakona koji su namijenjeni za oporavak, nisu bezbjedno zaštićeni od neovlašćenog pristupa i IKT kompromitacija i ako ne omogućavaju blagovremeno ponovno uspostavljanje usluga, pri čemu se, po potrebi, koriste rezervne kopije podataka i sistema (član 18 stav 6);
- 54) ne održava rezervne IKT kapacitete koji imaju resurse, sposobnosti i funkcije dovoljne za adekvatno obezbjeđivanje potreba poslovnih procesa (član 18 stav 7);
- 55) kao finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt nije procijenio potrebu održavanja rezervnih IKT kapaciteta iz člana 18 stav 7 ovog zakona (član 18 stav 8);
- 56) prilikom određivanja ciljnog vremena oporavka i ciljne tačke oporavka za svaku funkciju ne uzme u obzir značaj te funkcije, a naročito da li se radi o kritičnoj ili važnoj funkciji, kao i potencijalni ukupni uticaj ciljeva oporavka na efikasnost tržišta (član 18 st. 9 i 10);
- 57) prilikom oporavka od IKT incidenta ne sprovede sve neophodne kontrole, uključujući višestruke provjere i usklađivanja, kako bi obezbijedio održavanje najvišeg nivoa integriteta podataka (član 18 st. 11 i 12);
- 58) kao centralna druga ugovorna strana nema plan oporavka koji omogućava oporavak svih transakcija koje su bile u toku u trenutku nastanka poremećaja kako bi se obezbijedio nesmetan i siguran nastavak poslovanja centralne druge ugovorne strane i omogućilo izvršenje obaveze na predviđeni datum (član 18 stav 13);

- 59) kao pružalac usluga ne obezbijedi odgovarajuće resurse i infrastrukturu za izradu rezervnih kopija i obnovu sistema, radi kontinuiranog pružanja i održavanja svojih usluga (član 18 stav 14);
- 60) kao centralno klirinško depozitarno društvo ne održava najmanje jedno sekundarno mjesto obrade opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem, kako bi se zadovoljile poslovne potrebe (član 18 st. 15 i 16);
- 61) ne obezbijedi kapacitete ili ne odredi lica zadužena za prikupljanje informacija o ranjivostima, sajber prijetnjama ili IKT incidentima a naročito o sajber napadima, kao i za analizu njihovog mogućeg uticaja na digitalnu operativnu otpornost finansijskog subjekta (član 19 stav 1);
- 62) ne uspostavi ili ne sprovodi proces naknadne analize IKT incidenata koji se sprovodi nakon što značajan IKT incident poremeti obavljanje njegovih osnovnih aktivnosti, u cilju analize uzroka poremećaja i utvrđivanja potrebnih poboljšanja u IKT operacijama ili u IKT politici kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona (član 19 st. 2 i 4);
- 63) ne dostavi nadležnom organu, na njegov zahtjev, informacije o izmjenama koje su sprovedene nakon analize IKT incidenta iz člana 19 stav 2 ovog zakona (član 19 stav 3);
- 64) ne obezbijedi da se iskustva stečena kroz testiranje digitalne operativne otpornosti iz čl. 27 do 32 ovog zakona, kao i iz nastalih IKT incidenata, a naročito sajber napada, saznanja o izazovima koji su se pojavili prilikom pokretanja planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona, relevantne informacije dobijene od drugih subjekata, kao i informacije u vezi sa zahtjevima nadležnog organa, blagovremeno, adekvatno i kontinuirano koriste u okviru procesa procjene IKT rizika (član 19 stav 5);
- 65) iskustva, saznanja ili informacije iz člana 19 stav 5 ovog zakona na odgovarajući način ne uzima u obzir prilikom preispitivanja relevantnih komponenti sistema upravljanja IKT rizicima (član 19 stav 6);
- 66) ne prati efikasnost sprovođenja strategije digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona (član 19 stav 7);
- 67) ne evidentira ili ne prati promjenu ukupnog profila IKT rizika tokom vremena ili ne analizira učestalost, vrste, razmjere i trendove IKT incidenata, a naročito sajber napada i njihovih obrazaca, kako bi razumio nivo svoje izloženosti IKT riziku, posebno u odnosu na kritične ili važne funkcije i unaprijedio stepen svoje zrelosti i spremnosti u oblasti sajber bezbjednosti (član 19 stav 8);
- 68) ne osmisli ili ne sprovodi programe za podizanje svijesti o IKT bezbjednosti i obuke o digitalnoj operativnoj otpornosti kao obavezne djelove svojih programa obuke zaposlenih (član 19 st. 10 i 11);
- 69) kada je to primjenljivo, ne uključi treće strane koje pružaju IKT usluge u odgovarajuće programe obuke, u skladu sa članom 38 stav 3 tačka 11 ovog zakona (član 19 stav 12);
- 70) kontinuirano ne prati trendove u razvoju tehnologija kako bi bolje razumio mogući uticaj primjene novih tehnologija na zahtjeve u oblasti IKT bezbjednosti i digitalnu operativnu otpornost (član 19 stav 13);

- 71) nije upoznat sa najnovijim metodama za upravljanje IKT rizicima kako bi mogao efikasno da odgovori na postojeće i nove oblike sajber napada (član 19 stav 14);
- 72) u okviru sistema upravljanja IKT rizicima ne utvrdi planove komunikacije u kriznim situacijama, koji mu omogućavaju da na odgovoran način saopštava informacije najmanje o značajnim IKT incidentima i značajnim ranjivostima, klijentima, poslovnim partnerima i široj javnosti, u zavisnosti od slučaja (član 20 stav 1);
- 73) u okviru sistema upravljanja IKT rizicima ne utvrdi ili ne primjenjuje politike komunikacije za zaposlene ili sa eksternim zainteresovanim stranama (član 20 stav 2);
- 74) politikama komunikacije za zaposlene ili sa eksternim zainteresovanim stranama iz člana 20 stav 2 ovog zakona, u dijelu koji se odnosi na zaposlene, ne obezbijedi razlikovanje između zaposlenih koje je potrebno samo informisati i zaposlenih koji učestvuju u upravljanju IKT rizicima, odnosno koji su zaduženi za odgovor i oporavak (član 20 stav 3);
- 75) ne zaduži najmanje jedno lice u finansijskom subjektu za sprovođenje strategije komunikacije u slučaju IKT incidenata da u tu svrhu obavlja poslove informisanja medija i javnosti (član 20 stav 4);
- 76) kao finansijski subjekt koji u skladu sa članom 21 stav 1 primjenjuje pojednostavljeni sistem upravljanja IKT rizicima ne ispunjava zahtjeve propisane članom 21 stav 2 ovog zakona;
- 77) ne definiše ili ne uspostavi ili ne primijeni proces upravljanja IKT incidentima radi otkrivanja, upravljanja i obavještanja o IKT incidentima (član 22 stav 1);
- 78) ne evidentira sve IKT incidente ili ozbiljne sajber prijetnje (član 22 stav 2);
- 79) ne uspostavi adekvatne procedure i postupke kojima se obezbjeđuje da se, na dosljedan i objedinjen način postupa sa IKT incidentima, vrši njihovo praćenje i preduzimaju dalje mjere, kako bi se obezbijedilo da se osnovni uzroci IKT incidenata identifikuju, dokumentuju i tretiraju, radi sprečavanja ponavljanja takvih incidenata (član 22 stav 3);
- 80) u okviru procesa upravljanja IKT incidentima iz člana 22 stav 1 ovog zakona ne postupa na način propisan članom 22 stav 4 ovog zakona;
- 81) ne klasifikuje IKT incidente ili ne utvrdi njihov uticaj na osnovu kriterijuma propisanih članom 23 stav 1 ovog zakona;
- 82) ne klasifikuje sajber prijetnje kao ozbiljne na osnovu kritičnosti usluga koje su izložene riziku, uključujući u pogledu transakcija i operacija finansijskog subjekta, broja i/ili značaja klijenata izloženih tom riziku ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana izložena tom riziku i geografske rasprostranjenosti u smislu područja izloženih riziku (član 23 stav 2);
- 83) ne izvijesti nadležni organ o značajnom IKT incidentu (član 24 st. 1 do 5);
- 84) odmah, bez odlaganja, ne obavijesti klijente o značajnom IKT incidentu koji utiče na njihove finansijske interese ili o preduzetim mjerama za ublažavanje negativnih uticaja tog incidenta (član 24 stav 8);
- 85) ne obavijesti klijente, kada je to primjenljivo, o mjerama zaštite od ozbiljne sajber prijetnje koje mogu da preduzmu (član 24 stav 9);
- 86) u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, a u cilju procjene spremnosti za upravljanje IKT incidentima, identifikovanja slabosti, nedostataka i

- odstupanja u digitalnoj operativnoj otpornosti i blagovremenog sprovođenja korektivnih mjera, ne uspostavi, ne održava ili redovno ne preispituje program za testiranje digitalne operativne otpornosti (član 27 stav 1);
- 87) program za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona, kao dio okvira za upravljanje IKT rizicima nije efikasan ili sveobuhvatan ili ne sadrži niz procjena, testova, metodologija, praksi i alata koji se sprovode i primjenjuju u skladu sa čl. 28 do 31 ovog zakona (član 27 stav 2);
- 88) ne sprovodi program za testiranje digitalne operativne otpornosti primjenom pristupa zasnovanog na procjeni rizika, i ne vodi računa o promjenljivom karakteru IKT rizika, konkretnim rizicima kojima je izložen ili bi mogao biti izložen, kritičnosti informacione imovine i usluga, kao i o svim drugim relevantnim faktorima (član 27 stav 3);
- 89) ne obezbijedi da testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona sprovode nezavisna interna ili eksterna lica (član 27 stav 4);
- 90) u slučaju kada testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona sprovode interna lica ne obezbijedi dovoljne resurse za potrebe tog testiranja ili ne preduzme mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja tog testiranja (član 27 stav 5);
- 91) ne uspostavi politike i procedure za određivanje prioriteta, klasifikaciju i otklanjanje svih problema otkrivenih tokom testiranja digitalne operativne otpornosti ili ne uspostavi metodologije za internu provjeru radi dobijanja potvrde da su sve identifikovane slabosti, nedostaci i odstupanja u potpunosti otklonjeni (član 27 stav 6);
- 92) najmanje jednom godišnje ne sprovodi adekvatne testove svih IKT sistema i aplikacija koje podržavaju kritične ili važne funkcije tog finansijskog subjekta (član 27 stav 7);
- 93) programom za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona u skladu sa principom proporcionalnosti iz člana 5 ovog zakona ne obezbijedi sprovođenje odgovarajućih testova propisanih članom 28 stav 1 ovog zakona;
- 94) kao finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt ne sprovodi testiranja iz člana 28 stav 1 ovog zakona na način propisan članom 28 stav 2 ovog zakona;
- 95) kao centralno klirinško depozitarno društvo ili kao centralna druga ugovorna stana ne sprovodi procjene ranjivosti prije svake primjene ili ponovne primjene novih ili postojećih aplikacija, infrastrukturnih komponenti i IKT usluga koje podržavaju kritične ili važne funkcije finansijskog subjekta (član 28 stav 3);
- 96) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne sprovodi napredno testiranje u formi penetracionog testiranja vođenog prijetnjama najmanje jednom u tri godine (član 29 stav 1);
- 97) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne postupi po utvrđenoj obavezi promjene učestalosti naprednog testiranja (član 29 stav 2);
- 98) kao finansijski subjekt iz člana 29 stav 4 ovog zakona TLPT-om ne obuhvata više kritičnih ili važnih funkcija finansijskog subjekta ili sve takve funkcije, ili TLPT ne sprovodi na produkcionim sistemima koji podržavaju te funkcije (član 29 stav 3);
- 99) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne sprovede sve radnje potrebne za planiranje i sprovođenje TLPT-a propisane članom 29 stav 6 ovog zakona;

- 100) u slučaju kada su treće strane koje pružaju IKT usluge obuhvaćene TLPT-om, ne preduzme neophodne mjere i zaštitne mehanizme u skladu sa kojima se obezbjeđuje učešće tih trećih strana u TLPT-u (član 30 stav 1);
- 101) u saradnji sa trećim stranama koje pružaju IKT usluge, drugim uključenim stranama i licima koja sprovode testiranje ne primjeni efikasne kontrole upravljanja rizicima radi ublažavanja rizika od mogućih negativnih uticaja na podatke ili oštećenja imovine i poremećaja u obavljanju kritičnih ili važnih funkcija, usluga ili operacija (član 30 stav 6);
- 102) po završetku TLPT-a, nakon usaglašavanja izvještaja i planova za otklanjanje utvrđenih nedostataka, nadležnom organu, odnosno nadležnom organu kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona, ne dostavi rezime relevantnih nalaza ili planove za otklanjanje utvrđenih nedostataka ili dokumentaciju kojom se potvrđuje da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona (član 31 stav 1);
- 103) u slučaju da mu je potvrdu o sprovedenom TLPT-u izdao organ koji nije zadužen za njegov nadzor, ne obavijesti nadležni organ o dobijanju te potvrde, i uz obavještenje ne dostavi rezime relevantnih nalaza ili planove za otklanjanje nedostataka (član 31 stav 5).
- 104) za svako treće sprovođenje TLPT-a ne angažuje eksterna lica (član 32 stav 2);
- 105) ne obezbijedi da lica angažovana za sprovođenje TLPT-a ispunjavaju zahtjeve propisane članom 32 stav 3 ovog zakona;
- 106) u slučaju angažovanja internih lica za sprovođenje TLPT-a, ne obezbijedi da su pored zahtjeva iz člana 32 stav 3 ovog zakona, ispunjeni dodatni zahtjevi propisani članom 32 stav 4 ovog zakona;
- 107) ugovorom koji je zaključio sa eksternim licem koje sprovodi TLPT ne obezbijedi dobro upravljanje rezultatima TLPT-a i da bilo kakva obrada podataka u vezi sa tim, uključujući generisanje, izradu, agregiranje, skladištenje, izvještavanje, saopštavanje i uništavanje podataka, ne stvara rizike za tog finansijskog subjekta (član 32 stav 5);
- 108) ne upravlja IKT rizikom povezanim sa trećim stranama kao sastavnim dijelom IKT rizika, u okviru sistema upravljanja IKT rizicima iz člana 10 ovog zakona, u skladu sa principima propisanim članom 33 stav 1 ovog zakona;
- 109) ne usvoji ili redovno ne preispituje strategiju upravljanja IKT rizikom povezanim sa trećim stranama uzimajući u obzir strategiju IKT nabavke od više dobavljača iz člana 12 stav 3 ovog zakona, kada je to primjenljivo (član 33 stav 2);
- 110) strategijom upravljanja IKT rizikom povezanim sa trećim stranama iz člana 33 stav 2 ovog zakona ne obuhvati politiku korišćenja IKT usluga koje pružaju treće strane za podršku kritičnih ili važnih funkcija finansijskog subjekta, i ako tu politiku ne primjenjuje na pojedinačnoj i kada je to primjenljivo, na potkonsolidovanoj i konsolidovanoj osnovi (član 33 stav 3);
- 111) prije zaključivanja ugovora o korišćenju IKT usluga ne sprovede sve procjene, provjere i analize propisane članom 33 stav 5 ovog zakona (član 33 stav 5 i član 37 stav 1);

- 112) u okviru sistema upravljanja IKT rizicima, na pojedinačnoj, kao i na potkonsolidovanoj i konsolidovanoj osnovi, ne vodi ili ne ažurira registar informacija o svim ugovorima o korišćenju IKT usluga koje pružaju treće strane (član 34 stav 1);
- 113) informacije o ugovorima iz člana 34 stav 1 ovog zakona nisu evidentirane tako da se ugovori koji se odnose na IKT usluge za podršku kritičnih ili važnih funkcija razlikuju od ugovora koji se ne odnose na te funkcije (član 34 stav 2);
- 114) nadležnom organu, najmanje jednom godišnje, ne dostavi izvještaj o broju novih ugovora o korišćenju IKT usluga, kategorijama trećih strana koje pružaju IKT usluge, vrsti ugovora i IKT uslugama i funkcijama koje se pružaju (član 34 stav 3);
- 115) nadležnom organu, na njegov zahtjev, ne stavi na raspolaganje pojedine djelove ili cjelokupan registar informacija iz člana 34 stav 1 ovog zakona, uključujući i druge informacije koje su nadležnom organu potrebne za sprovođenje nadzora (član 34 stav 4);
- 116) blagovremeno ne obavijesti nadležni organ o svakom planiranom ugovoru u skladu sa kojim namjerava da koristi IKT usluge za podršku kritičnih ili važnih funkcija, kao i o svakoj funkciji koja je podržana ugovorom o korišćenju IKT usluga, a koja postane kritična ili važna funkcija (član 34 stav 5);
- 117) zaključi ugovor sa trećom stranom koja pruža IKT usluge, koja ne primjenjuje odgovarajuće standarde informacione bezbjednosti (član 35 st. 1 i 2);
- 118) radi ostvarivanja prava pristupa, sprovođenja provjera i revizija nad trećom stranom koja pruža IKT usluge, nije unaprijed odredio učestalost provjera i revizija, kao i oblasti u kojima će se iste sprovesti u skladu sa opšteprihvaćenim revizorskim standardima i, kada je to primjenljivo, zahtjevima nadležnog organa u pogledu primjene tih standarda (član 35 stav 3);
- 119) ne provjeri da li revizori, bilo da su interni, eksterni ili grupa revizora, posjeduju odgovarajuće vještine i znanja neophodna za efikasno sprovođenje relevantnih revizija i procjena, u slučaju da ugovor zaključen sa trećom stranom koja pruža IKT usluge iz člana 35 stav 1 ovog zakona obuhvata korišćenje IKT usluga koje podrazumijevaju visok stepen tehničke složenosti (član 35 stav 4);
- 120) nije obezbijedio da se ugovor o korišćenju IKT usluga može raskinuti u slučajevima propisanim članom 36 stav 1 ovog zakona;
- 121) nije utvrdio izlazne strategije za IKT usluge koje podržavaju kritične ili važne funkcije (član 36 st. 2 i 3);
- 122) nije obezbijedio da raskid ugovora sa trećom stranom koja pruža IKT usluge ne dovodi do posljedica propisanih članom 36 stav 4 ovog zakona;
- 123) ne obezbijedi da su planovi za raskid ugovornih odnosa iz člana 36 stav 1 ovog zakona sveobuhvatni, dokumentovani ili ne obezbijedi da se u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, dovoljno testiraju i periodično preispituju (član 36 stav 5);
- 124) nije utvrdio alternativna rješenja ili nije razvio tranzicione planove koji mu omogućavaju da, na siguran i cjelovit način, prenese ugovorene IKT usluge i povezane podatke sa treće strane koja pruža IKT usluge na alternativne pružaoce usluga ili ih

- reintegriše u okviru sopstvenih kapaciteta, kao i da obezbijedi njihovo uklanjanje kod treće strane koja je pružala IKT usluge (član 36 stav 6);
- 125) nije uspostavio odgovarajuće mjere za nepredviđene situacije radi očuvanja kontinuiteta poslovanja u slučaju nastanka okolnosti iz člana 36 stav 3 ovog zakona (član 36 stav 7);
- 126) ne procijeni prednosti i troškove alternativnih rješenja kao što je angažman različitih trećih strana koje pružaju IKT usluge, uzimajući u obzir da li i na koji način predviđena rješenja odgovaraju poslovnim potrebama i ciljevama utvrđenim u strategiji digitalne operativne otpornosti tog finansijskog subjekta (član 37 stav 2);
- 127) u slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, koji radi pružanja tih usluga, predviđa mogućnost treće strane koja pruža IKT usluge da kao podizvođače angažuje druge pružaoce IKT usluga, nije procijenio prednosti ili rizike koji mogu proizaći iz tog angažovanja, naročito u slučaju angažovanja IKT podizvođača sa sjedištem u trećoj zemlji (član 37 stav 3);
- 128) u slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, ne razmotri propise koji bi se primjenjivali u slučaju insolventnosti treće strane koja pruža IKT usluge, uključujući stečaj i likvidaciju, kao i sva ograničenja koja bi mogla nastati u slučaju potrebe za hitnim povratkom podataka finansijskog subjekta (član 37 stav 4);
- 129) u slučaju da se ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije zaključuje sa trećom stranom koja pruža IKT usluge sa sjedištem u trećoj zemlji, pored elemenata iz člana 37 stava 4 ovog zakona, ne razmotri i usklađenost sa odredbama propisa kojima se uređuje zaštita podataka, kao i mogućnost sprovođenja zakona u toj trećoj zemlji (član 37 stav 5);
- 130) u slučaju da je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđena mogućnost angažovanja podizvođača, ne procijeni da li, i na koji način, potencijalno dugi ili složeni lanci podugovaranja mogu uticati na njegovu sposobnost da u potpunosti prati ugovorene funkcije, kao i na mogućnost nadležnog organa da sprovodi efikasan nadzor tog finansijskog subjekta (član 37 stav 6);
- 131) nije utvrdio prava i obaveze strana u ugovoru (član 38 stav 1);
- 132) ugovor o pružanju IKT usluga nije dostupan ugovornim stranama u papirnom ili elektronskom obliku koji se može preuzeti u pristupačnom i trajnom formatu. (član 38 stav 2);
- 133) ugovor o korišćenju IKT usluga ne sadrži elemente propisane članom 38 stav 3 ovog zakona;
- 134) ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije pored elemenata iz člana 38 stav 3 ovog zakona ne sadrži dodatne elemente propisane članom 38 stav 4 ovog zakona (član 38 st. 4 i 5);
- 135) bez odlaganja ne obavijesti nadležni organ o svom učešću u sporazumima za razmjenu informacija iz člana 39 stav 1 tačka 3 ovog zakona, odnosno kada prestane sa učešćem u tom sporazumu (član 39 stav 3);
- 136) kao finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona ne postupi u skladu sa propisom Centralne banke iz člana 48 ovog zakona (član 48 stav 9);
- 137) kao finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona ne postupi u skladu sa propisom Komisije iz člana 49 ovog zakona (član 49 stav 10);

138) kao finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona ne postupi u skladu sa propisom Agencije iz člana 50 ovog zakona (član 50 stav 9);

139) kao finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona ne postupi u skladu sa propisom koji je nadležni organ iz člana 3 stav 1 tačka 4 ovog zakona donio u skladu sa članom 51 ovog zakona (član 51 stav 2);

140) ne sprovede mjeru koju je nadležni organ izrekao u skladu sa članom 40 st. 5 i 6 ovog zakona na način i u roku utvrđenim rješenjem o izricanju mjere (član 40 stav 7);

141) u potpunost ne sarađuje sa nadležnim organom tokom postupka nadzora ili kontrole i na zahtjev nadležnog organa za potrebe sprovođenja nadzora ili kontrole ne dostavi zahtijevana pisana ili usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole (član 40 stav 8);

(2) Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 2.000 eura do 4.000 eura.

(3) Novčanom kaznom u iznosu od 2.000 eura do 4.000 eura kazniće se za prekršaj član organa upravljanja finansijskog subjekta ako:

1) ne utvrdi, ne odobri ili ne nadzire sva pravila, postupke, procese, mehanizme, mjere i resurse povezane sa sistemom upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona i ne obezbijedi njihovu primjenu, i u tom cilju naročito ne ispuni uslove propisane članom 9 stav 3 ovog zakona;

2) aktivno ne unapređuje znanje i vještine potrebne za razumijevanje i procjenu IKT rizika i njegovog uticaja na poslovanje finansijskog subjekta uključujući i kroz redovne posebne obuke, srazmjerno prirodi rizika kojim se upravlja (član 9 stav 5);

3) ne obezbijedi da viši IKT kadar, najmanje jednom godišnje, podnosi izvještaj organu upravljanja o zaključcima izvedenim iz iskustava, saznanja i informacija iz člana 19 stav 5 ovog zakona, sa predlozima za dalje postupanje (član 19 stav 9);

4) na osnovu procjene ukupnog rizičnog profila finansijskog subjekta, obima i složenosti poslovnih usluga, redovno ne preispituje rizike identifikovane u vezi sa ugovorima o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije (član 33 stav 4).

XII. PRELAZNE I ZAVRŠNA ODREDBA

Rok za donošenje propisa

Član 53

Nadležni organi će u roku od 18 mjeseci od dana stupanja na snagu ovog zakona donijeti propise za čije donošenje su ovlašćeni čl. 48 do 51 ovog zakona.

Usklađivanje sa odredbama ovog zakona

Član 54

Finansijski subjekt je dužan da izvrši usklađivanje sa odredbama ovog zakona u roku od 24 mjeseca od dana stupanja na snagu ovog zakona.

Odložena primjena

Član 55

Odredbe člana 23 stav 1 tačka 3, člana 24 stav 11 tač. 1 i 2 i st. 12, 13 i 14, člana 29 stav 4 tačka 2 alineja 2, člana 31 stav 3 tačka 2 i stav 4, člana 32 stav 3 tačka 4, člana

38 stav 4 tačka 5 alineja 4, člana 45 st. 3 do 8 ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

Stupanje na snagu

Član 56

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore“.

** u ovaj zakon prenijete su odredbe Regulative (eu) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (tekst od značaja za EEP)*

OBRAZLOŽENJE

I. USTAVNI OSNOV

Ustavni osnov za donošenje Zakona o digitalnoj operativnoj otpornosti finansijskog sektora sadržan je u odredbama člana 16 tačka 5 Ustava Crne Gore, kojim je propisano da se zakonom, u skladu sa Ustavom, uređuju druga pitanja od interesa za Crnu Goru.

II. RAZLOZI ZA DONOŠENJE ZAKONA

Regulativa (EU) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (tekst od značaja za EEP) (u daljem tekstu: Regulativa (EU) 2022/2554), u Evropskoj uniji je stupila na snagu 16. januara 2023. godine, a primjenjuje se od 17. januara 2025. godine. Obzirom da u crnogorskom zakonodavnom okviru trenutno nema propisa kojim se vrši usaglašavanje sa ovom regulativom, donošenje Predloga zakona je ključni preduslov za zatvaranje Pregovaračkog poglavlja 9.

Ovim Predlogom zakona predlaže se zakon kojim se vrši usklađivanje nacionalnog zakonodavstva sa Regulativom (EU) 2022/2554. Njime se utvrđuju nadležni organi, ovlaštenja nadležnih organa, postupak nadzora, nadzorne mjere i prekršajne odredbe za kršenje odredbi ovog Predloga zakona.

Uzimajući u obzir da sve veća digitalizacija i međusobna povezanost povećavaju rizik informaciono-komunikacionih tehnologija (u daljem tekstu: IKT rizik), što društvo u cjelini, a posebno finansijski sistem, čini osjetljivijim na sajber prijetnje ili poremećaje u oblasti IKT-a, Predlogom zakona utvrđuju se jedinstveni zahtjevi u pogledu bezbjednosti mrežnih i informacionih sistema koji podržavaju poslovne procese finansijskih subjekata obuhvaćenih njegovim područjem primjene, kako bi se postigao visok zajednički nivo digitalne operativne otpornosti u finansijskom sektoru.

Stoga, radi očuvanja potpune kontrole nad IKT rizikom, finansijski subjekti obuhvaćeni područjem primjene Predloga zakona, u skladu sa njegovim odredbama, moraju imati sveobuhvatne kapacitete koji omogućavaju snažno i djelotvorno upravljanje IKT rizicima, kao i posebne mehanizme i politike za postupanje u vezi sa svim IKT incidentima i za izvještavanje o značajnim IKT incidentima. Takođe, finansijski subjekti obuhvaćeni područjem primjene Predloga zakona dužni su da uspostave politike za testiranje sistema, kontrola i procesa u oblasti IKT-a, kao i politike upravljanja IKT rizikom povezanim sa trećim stranama.

U skladu sa navedenim, Predlogom zakona se utvrđuju:

- zahtjevi primjenjivi na finansijske subjekte obuhvaćene njegovim područjem primjene, a koji se, između ostalog, odnose na upravljanje IKT rizikom, izvještavanje o značajnim IKT incidentima i dobrovoljno obavješćavanje nadležnih organa o

ozbiljnim sajber prijetnjama, testiranje digitalne operativne otpornosti i mjere za dobro upravljanje IKT rizikom povezanim sa trećim stranama;

- zahtjevi koji se odnose na ugovorne aranžmane između trećih strana pružalaca IKT usluga i finansijskih subjekata;
- pravila o saradnji između nadležnih organa i njihovoj saradnji sa drugim nacionalnim organima i organima Evropske unije;
- pravila o sprovođenju nadzora nad primjenom Predloga zakona i kaznene odredbe.

Cilj Predloga zakona je da konsoliduje i unaprijedi zahtjeve u pogledu IKT rizika kao dio zahtjeva u vezi sa operativnim rizikom, koji su do sada bili odvojeno razmatrani u različitim propisima. Iako su takvi propisi pokrivali glavne kategorije finansijskih rizika (npr. kreditni rizik, tržišni rizik, rizik druge ugovorne strane, rizik likvidnosti, rizik tržišnog ponašanja), u vrijeme njihovog donošenja nijesu sveobuhvatno obrađene sve komponente operativne otpornosti. Pravila o operativnim rizicima u sektorskim propisima često su se zasnivala na tradicionalnom kvantitativnom pristupu upravljanju rizikom (npr. određivanje kapitalnih zahtjeva za pokrivanje IKT rizika), te nijesu obuhvatala ciljana kvalitativna pravila u vezi sposobnosti zaštite, detekcije, ograničavanja, odgovora i oporavka u slučaju IKT incidenata, niti za izvještavanje i digitalno testiranje. Predlogom zakona se želi podići svijest o IKT rizicima i uvažiti činjenica da IKT incidenti i nedostatak operativne otpornosti mogu ugroziti stabilnost finansijskih subjekata.

Predlogom zakona stvara se regulatorni okvir za digitalnu operativnu otpornost, u okviru kojeg finansijski subjekti obuhvaćeni njegovim područjem primjene moraju obezbijediti otpornost na sve vrste poremećaja i prijetnji povezanih sa IKT-om, kao i sposobnost da na adekvatan način odgovore na takve poremećaje i obnove svoje poslovanje.

Područje primjene Predloga zakona široko je definisano i obuhvata finansijske subjekte navedene u članu 2.

Kako su subjekti iz člana 2 stav 5 tač. 4–23 Direktive 2013/36/EU isključeni iz njenog područja primjene, član 2 stav 4 Regulative (EU) 2022/2554 omogućava da se iz primjene ove Regulative isključe isti ti subjekti. U Crnoj Gori to je Razvojna banka Crne Gore. Zbog toga ovaj Predlog zakona predviđa da se on neće primjenjivati na Razvojnu banku Crne Gore.

Takođe, Predlog zakona predviđa odgovarajuća izuzeća i proporcionalnu primjenu njegovih odredbi u odnosu na finansijske subjekte koji su klasifikovani kao mikro finansijski subjekti, uzimajući u obzir njihovu veličinu, profil rizičnosti i složenost poslovanja.

U skladu sa Predlogom zakona, finansijski subjekti dužni su da uspostave sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima, kako bi se postigao visok nivo digitalne operativne otpornosti. Finansijski subjekti, u skladu sa sopstvenim sistemom za upravljanje IKT rizicima, dužni

su da uticaj IKT rizika svedu na najmanju moguću mjeru, primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata.

Krajnja odgovornost organa upravljanja za upravljanje IKT rizicima finansijskog subjekta predstavlja osnovno načelo ovog sveobuhvatnog pristupa, što podrazumijeva kontinuirani angažman organa upravljanja u nadzoru i praćenju upravljanja IKT rizicima. Finansijski subjekti dužni su nadležnom organu, na njegov zahtjev, da dostave potpune i ažurirane informacije o IKT rizicima i sopstvenom sistemu upravljanja IKT rizicima.

Na osnovu Predloga zakona finansijski subjekti dužni su da definišu, uspostave i sprovedu proces upravljanja IKT incidentima radi njihovog otkrivanja, upravljanja njima i izveštavanja o njima. Predlogom zakona se usklađuje sistem izveštavanja o IKT incidentima, uvodeći zahtjev da svi finansijski subjekti o značajnim IKT incidentima direktno izveštavaju svoje nadležne organe. Takav direktan model izveštavanja omogućava nadležnim organima neposredan pristup podacima o značajnim IKT incidentima.

Nadležni organi treba da prosljeđuju detalje o značajnim IKT incidentima organima utvrđenim zakonom kojim se uređuje informaciona bezbjednost (kao što je Agencija za sajber bezbjednost). Time se povećava nivo informisanosti takvih organa i omogućava, u slučaju nacionalnih CSIRT timova (Computer Security Incident Response Team), brza asistencija finansijskim subjektima kada je to potrebno.

Predlogom zakona se povećava nivo usklađenosti elemenata digitalne otpornosti uvođenjem strožih zahtjeva za upravljanje IKT rizicima i izveštavanje o IKT incidentima u odnosu na postojeće nacionalne propise u oblasti finansijskih usluga. Time se postiže veći stepen usklađenosti i u odnosu na zahtjeve utvrđene zakonom kojim se uređuje informaciona bezbjednost. Stoga se Predlog zakona smatra *lex specialis* propisom u odnosu na Zakon o informacionoj bezbjednosti („Sl. list Crne Gore“ br. 113/24).

Pored toga, Predlog zakona predviđa mogućnost da finansijski subjekti, na dobrovoljnoj osnovi, obavijeste nadležni organ o ozbiljnim sajber prijetnjama, ako smatraju da je prijetnja relevantna za finansijski sistem, korisnike usluga ili klijente.

Kako bi se postigao visok nivo digitalne operative otpornosti, u skladu sa relevantnim međunarodnim standardima i okvirima koji se primjenjuju u EU, poput TIBER-EU okvira, finansijski subjekti, u skladu sa Predlogom zakona, treba redovno da testiraju svoje IKT sisteme i zaposlene koji imaju odgovornosti u oblasti IKT-a, imajući u vidu njihove sposobnosti u pogledu sprečavanja, otkrivanja, odgovora i oporavka u slučaju napada i incidenata. Cilj testiranja je identifikacija i otklanjanje mogućih ranjivosti.

S obzirom na različite nivoe zrelosti i pripremljenosti finansijskih subjekata u domenu sajber bezbjednosti, testiranje obuhvata širok spektar metoda — od procjene osnovnih zahtjeva do naprednog testiranja zasnovanog na penetracionom testiranju vođenom prijetnjama (engl. Threat-Led Penetration Testing – TLPT). Takvo napredno

testiranje zahtijevaće se samo od onih finansijskih subjekata koji imaju adekvatan nivo IKT zrelosti da ga mogu sprovoditi na odgovarajući način.

Kako bi se u finansijskom sektoru obezbijedilo pouzdano praćenje IKT rizika povezanog sa trećim stranama, Predlogom zakona utvrđen je skup pravila zasnovanih na načelima, sa ciljem da se finansijskim subjektima pruže smjernice za praćenje rizika koji nastaje u kontekstu funkcija eksternalizovanih trećim stranama - pružaocima IKT usluga, posebno kada se radi o IKT uslugama koje podržavaju kritične ili važne funkcije, kao i uopšteno, u kontekstu svih vidova zavisnosti od trećih strana u oblasti IKT-a.

Pri tome, kako bi se uzela u obzir složenost različitih izvora IKT rizika, Predlog zakona obuhvata širok spektar trećih strana pružalaca IKT usluga. Definicija „kritične ili važne funkcije“ iz Predloga zakona obuhvata i pojam „kritičnih funkcija“ kako su definisane u članu 2 stav 1 tačka 35 Direktive 2014/59/EU Evropskog parlamenta i Savjeta od 15. maja 2014. o uspostavljanju okvira za oporavak i sanaciju kreditnih institucija i investicionih društava. U skladu sa navedenim, funkcije koje se smatraju kritičnim na osnovu Direktive 2014/59/EU uključene su u definiciju kritičnih funkcija u smislu Predloga zakona.

Finansijski subjekti bi trebalo da primjenjuju proporcionalan pristup praćenju rizika koji nastaju na nivou trećih strana - pružalaca IKT usluga, uzimajući u obzir prirodu, obim, složenost i značaj sopstvene zavisnosti od IKT usluga, kao i kritičnost ili važnost usluga, procesa ili funkcija koje su predmet ugovora. Na kraju, takav pristup treba da se zasniva na detaljnoj procjeni mogućeg uticaja na kontinuitet i kvalitet finansijskih usluga – kako na nivou pojedinačnog subjekta, tako i na nivou grupe, kada je to primjenjivo.

Pored toga, Predlogom zakona je uzeto u obzir da je finansijski ekosistem EU postao zavisn od određenih IKT usluga. Neki pružaoci takvih usluga predstavljaju ključne inovatore u razvoju i primjeni tehnologija zasnovanih na IKT-u i imaju važnu ulogu u pružanju finansijskih usluga, ili su se duboko integrisali u lanac vrijednosti finansijskih usluga. Time predstavljaju suštinski značaj za stabilnost i cjelovitost finansijskog sistema EU.

Shodno tome, na osnovu Regulative (EU) 2022/2554, takve kritične treće strane – pružaoci IKT usluga – su obuhvaćene posebnim nadzornim okvirom EU, s ciljem:

- unapređenja konvergencije i efikasnosti pristupa Evropskih nadzornih organa u upravljanju IKT rizicima povezanim sa trećim stranama u finansijskom sektoru,
- jačanja digitalne operativne otpornosti finansijskih subjekata koji se oslanjaju na kritične treće strane - pružaoce IKT usluga,
- i doprinosa očuvanju stabilnosti finansijskog sistema EU i cjelovitosti unutrašnjeg tržišta finansijskih usluga.

U skladu sa navedenim, Predlogom zakona su predviđene odredbe sa odloženom primjenom kojima se predviđa saradnja nacionalnih nadležnih organa sa EBA-om, ESMA-om i EIOPA-om u aktivnostima koje ti EU organi sprovode sa ciljem efikasne supevizije kritičnih trećih strana – pružalaca IKT usluga u EU.

Kako bi se obezbijedila primjena Predloga zakona u odnosu na finansijske subjekte obuhvaćene njenim područjem primjene, nadležni organi dobijaju niz ovlašćenja kojima se definišu njihove nove uloge i stalni zadaci, poput prikupljanja i analize podataka o značajnim IKT incidentima i učešća u sprovođenju međusektorskih sajber vježbi na nivou EU (odložena primjena).

Cilj Predloga zakona jeste jačanje ukupne digitalne operativne otpornosti finansijskog sektora i obezbjeđivanje da se korisnici mogu pouzdano osloniti na usluge finansijskih subjekata obuhvaćenih njenim područjem primjene, čak i u slučaju značajnih poremećaja.

Usklađenost sa Predlogom zakona obezbjeđivaće nadležni organi, u skladu sa ovlašćenjima utvrđenim zakonom. Propisane su odgovarajuće kazne i korektivne mjere radi obezbjeđivanja efikasnog sprovođenja odredbi Predloga zakona, u skladu sa zahtjevima Regulative (EU) 2022/2554, a naročito člana 50 stav 4.

III. USAGLAŠENOST SA PRAVNOM TEKOVINOM EVROPSKE UNIJE I POTVRĐENIM MEĐUNARODNIM KONVENCIJAMA

Predloženim zakonom izvršeno je potpuno usklađivanje sa Regulativom (EU) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011.

IV. OBJAŠNJENJE OSNOVNIH PRAVNIH INSTITUTA

Predlogom zakona se, u **Poglavlju I, u čl. 1 do 8** uređuju predmet i cilj zakona, područje njegove primjene i nadležnost organa koji sprovode nadzor nad primjenom zakona, kao i definicije osnovnih pojmova koji se koriste u daljem tekstu zakona. Ovo poglavlje predstavlja osnov za razumijevanje digitalne operativne otpornosti i utvrđuje da se zakon primjenjuje na širok spektar finansijskih subjekata, uz pojedine izuzetke.

U **Poglavlju II, u čl. 9 do 21**, propisuje se sistem upravljanja IKT rizicima koji obuhvata strateško planiranje, politiku bezbjednosti informacija, mjere za upravljanje incidentima, kontinuitet poslovanja, oporavak u vanrednim situacijama i procese obuke i nadzora. U ovom dijelu se detaljno uređuje način identifikovanja, praćenja i ublažavanja IKT rizika, kao i zahtjevi koji se odnose na interne kontrole, upravljanje pravima pristupa i mehanizmi za detekciju anomalija. Posebnim pravilima obuhvaćena je i mogućnost pojednostavljenog režima za mikro subjekte.

Poglavlje III, obuhvaćeno čl. 22 do 26, uređuje upravljanje IKT incidentima, njihovo klasifikovanje, način evidentiranja, obavezu prijavljivanja nadležnim organima i obavezu informisanja korisnika kada incident može uticati na njihove interese. U ovom

poglavlju se propisuje i razmjena informacija između nacionalnih nadzornih organa i evropskih tijela, posebno kada se radi o incidentima koji mogu imati prekogranični značaj.

Poglavlje IV, čl. 27 do 32, bavi se testiranjem digitalne operativne otpornosti. U njemu se utvrđuje i obaveza subjekata da razviju program testiranja, uključujući različite vrste tehničkih i organizacionih testova. Za subjekte od posebne važnosti uvodi se napredni oblik testiranja zasnovan na prijetnjama (TLPT), dok se za manje subjekte predviđaju proporcionalni zahtjevi. Posebno se uređuje način sprovođenja testova, dokumentovanja nalaza i postupanje po identifikovanim slabostima.

Poglavljem V, u čl. 33 do 38, uređuje se upravljanje IKT rizikom povezanim sa trećim stranama, uključujući dobavljače IKT usluga. U njemu se propisuju obaveze subjekata da procjenjuju rizike koji proističu iz ugovornih odnosa, da upravljaju rizikom koncentracije i da obezbijede da ugovori sadrže precizno definisane obaveze trećih strana u pogledu bezbjednosti, dostupnosti i integriteta podataka, uključujući uslove za podugovaranje, reviziju, prestanak usluga i povraćaj podataka.

U Poglavlju VI, u članu 39, uređuje se saradnja i razmjena informacija između subjekata o sajber prijetnjama, kao i obaveza izvještavanja nadležnih organa.

U Poglavlju VII, čl. 40 do 43, uređuje se nadzor nad primjenom zakona, uključujući ovlašćenja nadzornih organa, način vršenja supervizije i mjere koje se mogu preduzeti prema subjektima koji ne postupaju u skladu sa propisanim obavezama. U tim odredbama propisuju se i procedure saradnje, razmjene informacija i postupanja supervizora u slučaju utvrđenih nepravilnosti.

Poglavlje VIII, u čl. 44 i 45, reguliše način razmjene informacija između nadležnih organa, uključujući međusobnu saradnju domaćih supervizora i njihovu obavezu koordinisanja kada se radi o pitanjima od značaja za digitalnu operativnu otpornost. Propisuje se i obaveza razmjene podataka sa relevantnim evropskim tijelima, kako bi se obezbijedila usklađenost sa pravilima koja važe u državama članicama Evropske unije.

U poglavlju IX, u čl. 46 i 47, uređuje se obaveza čuvanja poslovne tajne i zaštite podataka o ličnosti u vezi sa podacima koji se prikupljaju, obrađuju i razmjenjuju u skladu sa ovim zakonom.

Poglavlje X, sadržano u čl. 48 do 51, propisuje ovlašćenja nadležnih organa da donose podzakonske propise radi bliže razrade tehničkih standarda, procedura izvještavanja, načina testiranja i drugih pitanja potrebnih za punu primjenu zakona.

Poglavlje XI sadrži prekršajne odredbe u članu 52, u kojima se utvrđuju povrede obaveza propisanih ovim zakonom, uključujući neprijavljivanje incidenata, nesprovođenje testiranja, nepropisno upravljanje trećim stranama i nepoštovanje obaveza u pogledu metapodataka, formata i rokova dostave.

Poglavlje XII, obuhvaćeno čl. 53 do 56, sadrži prelazne i završne odredbe, kojima se utvrđuju rokovi za donošenje podzakonskih propisa, rokovi za usklađivanje subjekata sa zakonom, odložena primjena pojedinih odredbi do pristupanja Crne Gore Evropskoj uniji, te odredba o stupanju na snagu zakona.

V. PROCJENA FINANSIJSKIH SREDSTAVA ZA SPROVOĐENJE ZAKONA

Za sprovođenje ovog zakona nijesu potrebna finansijska sredstva iz budžeta Crne Gore.

VI. RAZLOZI ZA DONOŠENJE ZAKONA PO HITNOM POSTUPKU

Ovaj zakon je potrebno donijeti po hitnom postupku, obzirom na zahtjeve EK u pogledu postizanja najvećeg mogućeg stepena usklađenosti crnogorskog zakonodavstva sa pravnom tekovinom EU, a u kontekstu ostvarivanja značajnog napretka u pregovaračkom procesu i zatvaranju Poglavlja 9 – Finansijske usluge.

IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	MINISTARSTVO FINANSIJA
NAZIV PROPISA	PREDLOG ZAKONA O DIGITALNOJ OPERATIVNOJ OTPORNOSTI FINANSIJSKOG SEKTORA
1. Definisanje problema - Koje probleme treba da riješi predloženi akt? - Koji su uzroci problema? - Koje su posljedice problema? - Koji su subjekti oštećeni, na koji način i u kojoj mjeri? - Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)? Finansijski sektor u Crnoj Gori je izložen sve većim operativnim i informacionim rizicima usljed ubrzane digitalizacije usluga, povećane upotrebe informacionih sistema, eksternih pružalaca IKT usluga i učestalih prekida, incidenata i potencijalnih napada na infrastrukturu. Trenutno ne postoji jedinstveni pravni okvir kojim bi se obezbijedio sistemski pristup upravljanju digitalnim operativnim rizicima, praćenju i prijavljivanju incidenata, otpornosti na poremećaje i koordinisanom odgovoru na IKT incidente u finansijskom sektoru. Uzroci problema su: - odsustvo jedinstvenog normativnog okvira za digitalnu operativnu otpornost, - porast zavisnosti od informacionih sistema i trećih pružalaca IKT usluga, - povećan broj i jačina operativnih i IKT incidenata, - međunarodna usklađivanja (EU propisi – DORA regulativa) koja zahtijevaju precizno uređenje ove oblasti. Posljedice trenutnog stanja su: fragmentiran pristup upravljanju IKT rizicima, nedovoljno jasne obaveze finansijskih institucija i pružalaca IKT usluga, neujednačeno izvještavanje o incidentima, viši operativni rizici i neusklađenost sa evropskim standardima. Nedonošenje ovog propisa negativno bi uticalo na finansijske institucije, posljedično i nadzorne organe, IKT pružaoce usluga, kao i krajnji korisnici finansijskih usluga koji su izloženi operativnim prekidima i potencijalnim sigurnosnim incidentima. Ukoliko bi se zadržao status quo, rizici po stabilnost i kontinuitet poslovanja finansijskih institucija bi rasli, a neusklađenost sa EU regulativom bi predstavljala prepreku daljem usklađivanju i pregovaračkom procesu.	
2. Ciljevi - Koji ciljevi se postižu predloženim propisom? - Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo. Propisom se postiže: - uspostavljanje jedinstvenog pravnog okvira digitalne operativne otpornosti finansijskog sektora,	

- usklađivanje domaćeg zakonodavstva sa relevantnim EU standardima u oblasti DORA,
- jačanje sistema upravljanja IKT rizicima u finansijskim institucijama,
- definisanje obaveza izveštavanja o incidentima, mjera preventivne zaštite i postupanja,
- uređenje nadzora i koordinacije između nadležnih organa i uspostavljanje nacionalnog okvira za upravljanje rizicima,
- stvaranje višeg nivoa zaštite stabilnosti finansijskog sistema.

Ciljevi su u skladu sa obavezama iz procesa pristupanja EU, kao i sa strateškim dokumentima iz oblasti finansijskih usluga, cyber bezbjednosti i digitalne transformacije.

3. Opcije

- Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa).
- Obrazložiti preferiranu opciju?

Opcija 1: Status quo

Zadržavanje postojećeg stanja ostavilo bi regulatorne praznine, nedovoljnu zaštitu sistema i značajne rizike po operativnu stabilnost finansijskog sektora. Neusklađenost sa EU propisima bi ostala.

Opcija 2: Neregulatorne mjere

Primjena preporuka, smjernica ili sektorskih uputstava bez donošenja zakona nije moguća, jer EU standardi zahtijevaju uspostavljanje formalnog normativnog okvira sa jasno definisanim obavezama i nadzorom.

Opcija 3: Donošenje zakona (preferirana opcija)

Propisuje obaveze finansijskih institucija i pružalaca ICT usluga, uređuje upravljanje rizicima, izveštavanje, nadzor i saradnju nadležnih organa. Ova opcija obezbjeđuje normativnu ujednačenost, punu usklađenost sa EU i unapređenu stabilnost sektora.

Preferirana je opcija 3 jer jedina omogućava ostvarenje ciljeva i minimiziranje operativnih rizika.

4. Analiza uticaja

- Na koga će i kako će najvjerojatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.
- Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima).
- Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.
- Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.
- Uključiti procjenu administrativnih opterećenja i biznis barijera.

Subjekti na koje propis utiče:

- definisane finansijske institucije;
- pružaoci IKT usluga koji obavljaju poslove za finansijske institucije,
- nadležni organi.

Pozitivni uticaji:

- jačanje digitalne operativne otpornosti finansijskih institucija,
- jasne obaveze u upravljanju IKT rizicima, testiranju otpornosti i izveštavanju o incidentima,

- unaprijeđena koordinacija nadzornih organa,
- bolja zaštita korisnika finansijskih usluga,
- povećana stabilnost i otpornost finansijskog sektora.

Negativni uticaji:

Potrebno je prilagođavanje internih procedura finansijskih institucija i pružalaca ICT usluga, ali se ne očekuju značajni negativni efekti.

Propis ne uvodi nove takse niti namete. Moguća su ograničena ulaganja institucija u jačanje sistema upravljanja IKT rizicima, ali to su dio standardnih operativnih obaveza i ne predstavljaju dodatne administrativne barijere.

Propis ne stvara direktne prepreke konkurenciji niti ograničava tržište. Stvara stabilnije regulatorno okruženje za finansijske i IKT subjekte.

Administrativna opterećenja se ne povećavaju na način koji bi predstavljao barijeru poslovanju.

Pozitivni efekti propisa nesumnjivo prevazilaze troškove usklađivanja.

5. Procjena fiskalnog uticaja

- Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?
- Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Obrazložiti.
- Da li implementacijom propisa proizilaze međunarodne finansijske obaveze? Obrazložiti.
- Da li su neophodna finansijska sredstva obezbijeđena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskalnu godinu?
- Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteci finansijske obaveze?
- Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?
- Obrazložiti metodologiju koja je korišćena prilikom obračuna finansijskih izdataka/prihoda.
- Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda? Obrazložiti.
- Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?
- Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.

Za implementaciju zakona nijesu potrebna budžetska sredstva iz Budžeta Crne Gore, niti se stvaraju nove međunarodne finansijske obaveze.

Propis ne stvara prihode za budžet.

Propis je rađen u okviru aktivnosti Radne grupe, formirane od strane Centralne banke, a čiji članovi su bili predstavnici Ministarstva finansija, Agencije za nadzor osiguranja i Komisije za tržište kapitala. Svi komentari članova radne grupe uključeni su u tekst propisa.

6. Konsultacije zainteresovanih strana

- Naznačiti da li je korišćena eksterna ekspertna podrška i ako da, kako.
- Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).
- Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.

Za pripremu ovog propisa nije korišćena eksterna ekspertska podrška.

Nacrt zakona bio stavljen na javnu raspravu, nakon koje je utvrđen konačan tekst.

Javna rasprava trajala je u periodu od 04.12.2025. do 23.12.2025. godine.

Izveštaj sa javne rasprave dostupan je na linku <https://www.gov.me/clanak/izvjestaj-o-sprovedenoj-javnoj-raspravi-za-nacrt-zakona-o-digitalnoj-operativnoj-otpornosti-finansijskog-sektora>.

7. Monitoring i evaluacija

- Koje su potencijalne prepreke za implementaciju propisa?
- Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?
- Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?
- Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?

Potencijalne prepreke u primjeni ovog propisa mogu biti: operativno prilagođavanje institucija novim standardima, potreba za koordinacijom nadležnih organa, uspostavljanje mehanizama za praćenje IKT incidenata.

Mjere za sprovođenje ovog propisa su kontinuirani nadzor nadležnih organa, uspostavljanje sistema izvještavanja i praćenja incidenata, izrada podzakonskih propisa i smjernica za primjenu normi gdje je potrebno.

Indikatori uspješnosti mogu biti:

- efikasno upravljanje IKT rizicima,
- uredno i pravovremeno izvještavanje o incidentima,
- smanjenje operativnih prekida i povećana otpornost sistema,
- pozitivna ocjena usklađenosti sa EU.

Nadležni organi za sprovođenje ovog propisa su Centralna banka, Komisija za tržište kapitala, Agencija za nadzor osiguranja u skladu sa zakonom.

Datum i mjesto

13.01.2026.





Crna Gora
Ministarstvo evropskih poslova

Adresa: Bulevar Ivana Crnojevića 167
81 000 Podgorica, Crna Gora
Tel: +382 20 481 301
www.gov.me/mep

Br: 04/4-907/26-43/2

15. januar 2026.

Za: MINISTARSTVO FINANSIJA

ministru Novici Vukoviću

Veza: Dopis br: 05/1-03-040/25-46653/6

**Predmet: Mišljenje o usklađenosti Predloga zakona o digitalnoj operativnoj otpornosti
finansijskog sektora s pravnom tekovinom EU**

Poštovani,

Dopisom broj 05/1-03-040/25-46653/6 od 13. januara 2025. godine tražili ste mišljenje o usklađenosti **Predloga zakona o digitalnoj operativnoj otpornosti finansijskog sektora** s pravnom tekovinom Evropske unije.

Nakon upoznavanja sa sadržinom predloga propisa, a u skladu sa nadležnostima definisanim članom 40 stav 1 alineja 2 Poslovnika Vlade Crne Gore („Sl. list CG“, br. 3/12, 31/15, 48/17, 62/18, 121/23, 58/24 i 43/25) Ministarstvo evropskih poslova je saglasno sa navodima u obrascu usklađenosti predloga propisa s pravnom tekovinom Evropske unije.

S poštovanjem,

Majda Gorčević
MINISTARKA EVROPSKIH POSLOVA

Prilog:

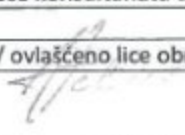
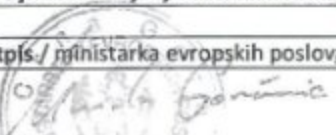
- Izjava i tabela usklađenosti Predloga zakona o digitalnoj operativnoj otpornosti finansijskog sektora s pravnom tekovinom EU

Dostavljeno:

- Ministarstvu finansija;
- a/a

**IZJAVA O USKLAĐENOSTI NACRTA/PREDLOGA PROPISA CRNE GORE
S PRAVNOM TEKOVINOM EVROPSKE UNIJE**

Identifikacioni broj Izjave		MF- IU/PZ/26/07
1. Naziv nacrt/predloga propisa		
- na crnogorskom jeziku	Predlog zakona o digitalnoj operativnoj otpornosti finansijskog sektora	
- na engleskom jeziku	Proposal of the Law on Digital Operational Resilience of the Financial Sector	
2. Podaci o obrađivaču propisa		
a) Organ državne uprave koji priprema propis		
Organ državne uprave	Ministarstvo finansija	
- Sektor/odsjek	Direktorat za finansijski sistem i koordinaciju politika	
- odgovorno lice (ime, prezime, telefon, e-mail)	Novica Vuković, ministar, novica.vukovic@mif.gov.me , +38220242835 Aleksandra Popović, generalna direktorica, aleksandra.popovic@mif.gov.me , +38263262818	
- kontakt osoba (ime, prezime, telefon, e-mail)	Aleksandra Popović, generalna direktorica, aleksandra.popovic@mif.gov.me , +38263262818	
b) Pravno lice s javnim ovlaštenjem za pripremu i sprovođenje propisa		
- Naziv pravnog lica	Centralna banka Crne Gore	
- odgovorno lice (ime, prezime, telefon, e-mail)	dr. Irena Radović, guvernerka kabinet@cbcg.me +38220403122 Milan Remiković, Viceguverner milan.remikovic@cbcg.me +38220403116	
- kontakt osoba (ime, prezime, telefon, e-mail)	Nikola Bašanović, koordinator Sektora za kontrolu nikola.basanovic@cbcg.me +38220403109	
3. Organi državne uprave koji primjenjuju/sprovođe propis		
- Organ državne uprave	Ministarstvo finansija i Centralna banka Crne Gore	
4. Usklađenost nacrt/predloga propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropske unije i njenih država članica, s jedne strane i Crne Gore, s druge strane (SSP)		
a) Odredbe SSPa s kojima se usklađuje propis		
Glava VIII, Politike saradnje, Član 91, Bankarstvo, osiguranje i druge finansijske usluge		
b) Step en ispunjenosti obaveza koje proizilaze iz navedenih odredbi SSPa		
	☒	ispunjava u potpunosti
	☐	djelimično ispunjava
	☐	ne ispunjava
c) Razlozi za djelimično ispunjenje, odnosno neispunjenje obaveza koje proizilaze iz navedenih odredbi SSPa		
/		
5. Veza nacrt/predloga propisa s programom pristupanja Crne Gore Evropskoj uniji (PPCG)		
- PPCG za period	2025-2026	
- Poglavlje, potpoglavlje	/	
- Rok za donošenje propisa	/	

- Napomena	Donošenje Zakona o digitalnoj operativnoj otpornosti finansijskog sektora nije predviđeno Programom pristupanja Crne Gore Evropskoj uniji.
6. Usklađenost nacrt/predloga propisa s pravnom tekovinom Evropske unije	
a) Usklađenost s primarnim izvorima prava Evropske unije	
UFEU, Dio treći – Politike i unutrašnje djelovanje Unije, Glava IV – Slobodno kretanje ljudi, usluga i kapitala, Poglavlje 3 – Usluge, član 58/TFEU, Article 58	
Potpuno usklađeno/Fully harmonized	
b) Usklađenost sa sekundarnim izvorima prava Evropske unije	
32022R2554	
Regulativa (EU) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011	
Djelimično usklađeno/Partly harmonized	
c) Usklađenost s ostalim izvorima prava Evropske unije	
Ne postoji izvor prava EU ove vrste sa kojim bi se nacrt propisa mogao uporediti radi ocjene stepena njegove usklađenosti.	
6.1. Razlozi za djelimičnu usklađenost ili neusklađenost nacrt/predloga propisa Crne Gore s pravnom tekovinom Evropske unije i rok u kojem je predviđeno postizanje potpune usklađenosti	
Predlog zakona o digitalnoj operativnoj otpornosti finansijskog sektora je skoro u potpunosti usklađen sa Regulativom (EU) 2022/2554. Manji broj odredbi ove regulative koji se odnosi na obuhvat primjene zakona, obaveze EU nadležnih organa u okviru sistema SSM, odnosi i obaveze tih organa prema SRB, zatim odredbe koje se odnose na ovlaštenja i obaveze EU tijela i institucija (naročito odredbe Poglavlja V Odjeljka 2 Regulative) nijesu u potpunosti prenesene zbog nemogućnosti primjene tih odredbi u Crnoj Gori. Potpuno usklađivanje sa ovim odredbama će biti izvršeno u narednoj fazi usklađivanja po pristupanju Crne Gore EU, dok će potpuno usklađivanje sa odredbom člana 16 stav 2 Regulative biti izvršeno kroz podzakonski akt na osnovu pravnog osnova iz člana 49 stav 9 Predloga zakona (sa rokom donošenja u 2 kvartal 2027. godine).	
7. Ukoliko ne postoje odgovarajući propisi Evropske unije s kojima je potrebno obezbijediti usklađenost konstatovati tu činjenicu	
/	
8. Navedi pravne akte Savjeta Evrope i ostale izvore međunarodnog prava korišćene pri izradi nacrt/predloga propisa	
Ne postoje izvori međunarodnog prava s kojima je / potrebno uskladiti predlog propisa.	
9. Navedi da li su navedeni izvori prava Evropske unije, Savjeta Evrope i ostali izvori međunarodnog prava prevedeni na crnogorski jezik (prevode dostaviti u prilogu)	
Regulativa 32022R2554 nije prevedena na crnogorski jezik.	
10. Navedi da li je nacrt/predlog propisa iz tačke 1 Izjave o usklađenosti preveden na engleski jezik (prevod dostaviti u prilogu)	
Predlog zakona o digitalnoj operativnoj otpornosti finansijskog sektora je preveden na engleski jezik.	
11. Učešće konsultanata u izradi nacrt/predloga propisa i njihovo mišljenje o usklađenosti	
/	
Potpis / ovlašteno lice obrađivača propisa	Potpis / ministarka evropskih poslova
	
Datum: 2026. godine	Datum:

Prilog obrasca:

1. Prevodi propisa Evropske unije
2. Predlog nacrt/predloga propisa na engleskom jeziku

TABELA USKLAĐENOSTI

1. Identifikacioni broj (IB) nacrt/predloga propisa		1.1. Identifikacioni broj izjave o usklađenosti i datum utvrđivanja nacrt/predloga propisa na Vladi		
MF-TU/PZ/26/07		MF-IU/PZ/26/07		
2. Naziv izvora prava Evropske unije i CELEX oznaka				
Regulativa (EU) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (Tekst od značaja za EEP) – 32022R2554				
3. Naziv nacrt/predloga propisa Crne Gore				
Na crnogorskom jeziku		Na engleskom jeziku		
Nacrt zakona o digitalnoj operativnoj otpornosti finansijskog sektora		Draft law on digital operational resilience for the financial sector		
4. Usklađenost nacrt/predloga propisa sa izvorima prava Evropske unije				
a)	b)	c)	d)	e)
Odredba i tekst odredbe izvora prava Evropske unije (član, stav, tačka)	Odredba i tekst odredbe nacrt/predloga propisa Crne Gore (član, stav, tačka)	Usklađenost odredbe nacrt/predloga propisa Crne Gore sa odredbom izvora prava Evropske unije	Razlog za djelimičnu usklađenost ili neusklađenost	Rok za postizanje potpune usklađenosti
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 finansijskih subjekata kako slijedi: (a) zahtjevi primjenjivi na finansijske 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 finansijskih subjekata iz članka 2. stavka 1. točaka od (a) do (d), o značajnim	I. OSNOVNE ODREDBE Predmet Član 1 Ovim zakonom utvrđuju se zahtjevi, postupci i mjere za obezbjeđivanje visokog nivoa digitalne operativne otpornosti finansijskog sektora, uključujući zahtjeve za bezbjednost mrežnih i informacionih sistema koji podržavaju poslovanje finansijskih subjekata, kao i druga pitanja od značaja za digitalnu operativnu otpornost finansijskog sektora.	Potpuno usklađeno		

operativnim ili sigurnosnim incidentima povezanim s plaćanjem; iv. testiranje digitalne operative 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 finansijskih subjekata; (c) pravila za uspostavu i provedbu nadzornog okvira za ključne treće strane pružatelje IKT usluga pri pružanju usluga finansijskim 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 finansijskim 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.	Nema odgovarajuće odredbe	Potpuno usklađeno	Materija je regulisana članom 1 Zakona o informacionoj bezbjednosti ("Službeni list Crne Gore", br. 113/24)	
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.	Član 2, stav 3 (3) Ovaj zakon ne utiče na odredbe zakona kojim se uređuju nadležnosti državnih organa u vezi sa zaštitom javne bezbjednosti, nacionalne bezbjednosti i odbrane.	Potpuno usklađeno		
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;	Primjena Član 2, stav 1 (1) Ovaj zakon primjenjuje se na subjekte finansijskog sektora (u daljem tekstu: finansijski subjekt), i to: 1) kreditnu instituciju; 2) platnu instituciju sa sjedištem u Crnoj Gori;	Potpuno usklađeno	Usklađivanje izvršeno za sve subjekte sa liste koji postoje u Crnoj Gori	

(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 kriptovalutinom koji imaju odobrenje za rad na temelju uredbe Europskog parlamenta i Vijeća o tržištima kriptovalutina i izmjeni uredaba (EU) br. 1093/2010 i (EU) br. 1095/2010 te direktiva 2013/36/EU i (EU) 2019/1937 („Uredba o tržištima kriptovalutina“) 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.	3) registrovanog pružaoca usluge informacija o računu sa sjedištem u Crnoj Gori; 4) instituciju za elektronički novac sa sjedištem u Crnoj Gori; 5) investiciono društvo; 6) centralno klirinško depozitarno društvo; 7) centralnu drugu ugovornu stranu; 8) mjesto trgovanja; 9) trgovinski repozitorij; 10) društvo za upravljanje alternativnim investicionim fondom; 11) društva za upravljanje otvorenim investicionim fondom sa javnom ponudom; 12) instituciju za profesionalnu penzionu štednju; 13) pružaoca usluga dostave podataka; 14) administratora ključnih referentnih vrijednosti; 15) društvo za osiguranje; 16) društvo za reosiguranje; 17) podružnicu stranog društava za osiguranje; 18) podružnicu stranog društava za reosiguranje; 19) društvo za posredovanje u osiguranju; 20) sporednog posrednika u osiguranju; 21) preduzetnika posrednika u osiguranju; 22) društvo za zastupanje u osiguranju; 23) sporednog zastupnika u osiguranju; 24) preduzetnika zastupnika u osiguranju; 25) agenciju za pružanje drugih usluga u osiguranju; 26) pružaoca usluga povezanih sa kriptovalutinom; 27) izdavaoca tokena vezanih za imovinu.		Određbe Regulative 2022/2554 koje se direktno odnose na kritične treće strane koje pružaju IKT usluge su neprenosive (Poglavlje V odjeljak II - Nadzorni okvir za kritične treće strane koje pružaju IKT usluge) Odrađen je reg. maksimum, dalje usklađivanje je moguće samo po pristupanju.	
2. Za potrebe ove Uredbe subjekti iz stavka 1. točaka od (a) do (t) zajednički se nazivaju „financijski subjekti“.	Član 2, stav 1 (1) Ova zakon primjenjuje se na subjekte finansijskog sektora (u daljem tekstu: finansijski subjekt), i to: 1) kreditnu instituciju; 2) platnu instituciju sa sjedištem u Crnoj Gori; 3) registrovanog pružaoca usluge informacija o računu sa sjedištem u Crnoj Gori; 4) instituciju za elektronički novac sa sjedištem u Crnoj Gori;	Potpuno usklađeno	Usklađivanje izvršeno za sve subjekte sa liste koji postoje u Crnoj Gori Odrađen je reg. maksimum, dalje	

	5) investiciono društvo; 6) centralno klirinško depozitarno društvo; 7) centralnu drugu ugovornu stranu; 8) mjesto trgovanja; 9) trgovinski repozitorij; 10) društvo za upravljanje alternativnim investicionim fondom; 11) društva za upravljanje otvorenim investicionim fondom sa javnom ponudom; 12) instituciju za profesionalnu penzionu štednju; 13) pružaoca usluga dostave podataka; 14) administratora ključnih referentnih vrijednosti; 15) društvo za osiguranje; 16) društvo za reosiguranje; 17) podružnicu stranog društava za osiguranje; 18) podružnicu stranog društava za reosiguranje; 19) društvo za posredovanje u osiguranju; 20) sporednog posrednika u osiguranju; 21) preduzetnika posrednika u osiguranju; 22) društvo za zastupanje u osiguranju; 23) sporednog zastupnika u osiguranju; 24) preduzetnika zastupnika u osiguranju; 25) agenciju za pružanje drugih usluga u osiguranju; 26) pružaoca usluga povezanih sa kriptovalutama; 27) izdavaoca tokena vezanih za imovinu.		usklađivanje je moguće samo po pristupanju.	
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;	Član 2, stav 2 (2) Ovaj zakon ne primjenjuje se na: 1) Razvojnu banku Crne Gore; 2) društva za osiguranje i društva za reosiguranje iz člana 3 i 4 Zakona o osiguranju ("Službeni list CG", broj 33/25); 3) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju koji su klasifikovani kao mikro, mali ili srednji finansijski subjekti; 4) institucije za profesionalnu penzionu štednju koje upravljaju penzionim šemama sa ukupno najviše 15 članova,	Potpuno usklađeno	Usklađivanje izvršeno za sve subjekte sa liste koji postoje u Crnoj Gori Odrađen je reg. maksimum, dalje usklađivanje je moguće samo po pristupanju.	

(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.	a koje su uređene zakonom kojim se uređuju dobrovoljni penzioni fondovi.			
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 obavještuje Komisiju. Komisija te informacije objavljuje na svojim internetskim stranicama ili na drugi lako dostupan način.	Član 2, stav 2, tačka 1 (2) Ovaj zakon ne primjenjuje se na: 1) Razvojnu banku Crne Gore; Saradnja sa organima Evropske unije i organima trećih država Član 45, stav 8 tačka 1 (8) Nadležni organ je dužan da obavještava Evropsku komisiju EBA-u, ESMA-u i EIOPA-u o: 1) propisima kojima se bliže uređuju zahtjevi iz ovog zakona, kao i o izmjenama tih propisa u rokovima propisanim Regulativom (EU) 2022/2554; 2) informacijama koje se razmjenjuju sa pravosuđnim organima i organima nadležnim za sprovođenje krivičnih sankcija u skladu sa članom 42 ovog zakona.	Potpuno usklađeno		
Članak 3. Definicije Za potrebe ove Uredbe primjenjuju se sljedeće definicije: 1. „digitalna operativna otpornost” znači sposobnost finansijskog 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 finansijski subjekt koristi i kojima se podupire kontinuirano pružanje finansijskih 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;	Digitalna operativna otpornost Član 4 Digitalna operativna otpornost, u smislu ovog zakona, je sposobnost finansijskog subjekta da izgradi, obezbijedi i preispituje svoj operativni integritet i pouzdanost, na način da, direktno ili indirektno kroz korišćenje usluga koje pružaju treće strane, odnosno pružaoci usluga informaciono komunikacionih tehnologija (u daljem tekstu: IKT), stvara uslove za primjenu svih IKT kapaciteta neophodnih za bezbjednost mrežnih i informacionih sistema koje koristi i koji podržavaju kontinuirano pružanje finansijskih usluga tog subjekta i očuvanje njihovog kvaliteta, uključujući i u slučaju poremećaja. Značenje izraza Član 8, stav 1, tačka 1 Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja: 1) mrežni i informacioni sistem je:	Potpuno usklađeno		
		Potpuno usklađeno		

	- elektronska komunikaciona mreža, odnosno sistem prenosa koji se zasniva na stalnoj infrastrukturi ili centralizovanom upravljačkom kapacitetu i obuhvata, gdje je primjenljivo, uređaje za komutaciju ili usmjeravanje i druga sredstva, uključujući pasivne mrežne elemente, koji omogućavaju prenos signala pomoću žičanih, radio, optičkih ili drugih elektromagnetnih sistema, uključujući satelitske mreže, fiksne (sa komutacijom kola i paketa, uključujući internet) i mobilne mreže, elektroenergetske kablovske sisteme, u dijelu koji se koristi za prenos signala, mreže koje se koriste za prenos i distribuciju radijskih i televizijskih programa bez obzira na vrstu informacije koja se prenosi; - svaki uređaj ili skup povezanih ili međuzavisnih uređaja, od kojih najmanje jedan programski izvršava automatsku obradu podataka u elektronskom obliku; ili - podaci u elektronskom obliku koji se čuvaju, obrađuju, dobijaju ili prenose na način iz al. 1 i 2 ove tačke, u svrhu rada, korišćenja, zaštite i održavanja tih mrežnih i informacionih sistema;			
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 finansijskog subjekta;	Član 8, stav 1, tačka 2 2) zastarjeli IKT sistem je IKT sistem koji je dostigao kraj svog životnog ciklusa, a koji zbog tehnoloških ili komercijalnih razloga nije pogodan za nadogradnje ili popravke ili za koji njegov dobavljač ili treća strana koja pruža IKT usluge prestane da pruža podršku, ali je i dalje u upotrebi i podržava funkcije finansijskog subjekta;	Potpuno usklađeno		
4. „sigurnost mrežnih i informacionih sustava“ znači sigurnost mrežnih i informacionih sustava kako je definirana u članku 6. točki 2. Direktive (EU) 2022/2555;	Član 8, stav 1, tačka 3 3) bezbjednost mrežnih i informacionih sistema je sposobnost mrežnih i informacionih sistema da se, na određenom nivou pouzdanosti, odupru svakom događaju koji može da ugrozi dostupnost, autentičnost, integritet ili povjerljivost podataka koji se čuvaju, prenose ili obrađuju, kao i usluga koje ti sistemi nude ili kojima se preko njih pristupa;	Potpuno usklađeno		
5. „IKT rizik“ znači svaka razumno prepoznatljiva okolnost koja se odnosi na upotrebu mrežnih i informacionih sustava, koja, ako do nje dođe, može dovesti do negativnih učinaka u digitalnom ili fizičkom okruženju te time ugroziti sigurnost mrežnih i informacionih sustava;	Član 8, stav 1, tačka 4 4) IKT rizik je svaka razumno prepoznatljiva okolnost koja se odnosi na korišćenje mrežnih i informacionih sistema, a koja, ukoliko nastane, može da dovede do negativnih uticaja u digitalnom ili fizičkom okruženju i ugrozi bezbjednost mrežnih i informacionih	Potpuno usklađeno		

informatičkih sustava, svih alata ili procesa koji ovise o tehnologiji, operacija i procesa ili pružanja usluga;	sistema, bilo kog tehnološki zavisnog alata ili procesa, poslovnih operacija i procesa ili pružanja usluga;			
6. „informatička imovina” znači skup materijalnih ili nematerijalnih informacija koje vrijedi zaštititi;	Član 8, stav 1, tačka 5 5) informaciona imovina je skup materijalnih ili nematerijalnih informacija, koje je potrebno zaštititi;	Potpuno usklađeno		
7. „IKT imovina” znači softverska ili hardverska imovina u mrežnim i informatičkim sustavima koju upotrebljava financijski subjekt;	Član 8, stav 1, tačka 6 6) IKT imovina je softverska ili hardverska imovina u mrežnim i informacionim sistemima koje koristi financijski subjekt;	Potpuno usklađeno		
8. „IKT incident” znači događaj ili niz povezanih događaja koje financijski subjekt nije planirao i koji ugrožavaju sigurnost mrežnih i informatičkih sustava i negativno utječu na dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka, ili na usluge koje pruža financijski subjekt;	Član 8, stav 1, tačka 7 7) IKT incident je jedan ili više povezanih događaja koje financijski subjekt nije planirao, a koji narušavaju bezbjednost mrežnih i informacionih sistema i negativno utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka, ili na usluge koje financijski subjekt pruža;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 8 8) operativni ili sigurnosni incident povezan sa plaćanjem je jedan ili više povezanih događaja, bez obzira da li su povezani sa IKT-om, koje financijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona nije planirao, a koji negativno utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka povezanih sa plaćanjem, ili na usluge povezane sa plaćanjem koje financijski subjekt pruža;	Potpuno usklađeno		
10. „značajan IKT incident” znači IKT incident koji izrazito negativno utječe na mrežne i informatičke sustave kojima se podupiru ključne ili važne funkcije financijskog subjekta;	Član 8, stav 1, tačka 9 9) značajan IKT incident je IKT incident koji ima visok nivo negativnog uticaja na mrežne i informacione sisteme koji podržavaju kritične ili važne funkcije financijskog subjekta;	Potpuno usklađeno		
11. „značajan operativni ili sigurnosni incident povezan s plaćanjem” znači operativni ili sigurnosni incident koji izrazito negativno utječe na pružene usluge povezane s plaćanjem;	Član 8, stav 1, tačka 10 10) značajan operativni ili sigurnosni incident povezan sa plaćanjem je operativni ili sigurnosni incident povezan sa plaćanjem koji ima visok nivo negativnog uticaja na usluge povezane sa plaćanjem koje se pružaju;	Potpuno usklađeno		
12. „kiberprijetnja” znači kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;	Član 8, stav 1, tačka 11 11) sajber prijetnja je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na mrežne i informacione sisteme, korisnike tih sistema i druga lica;	Potpuno usklađeno		

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;	Član 8, stav 1, tačka 12 12) ozbiljna sajber prijetnja je sajber prijetnja čije tehničke karakteristike ukazuju na to da bi mogla dovesti do značajnog IKT incidenta ili značajnog operativnog ili sigurnosnog incidenta povezanog sa plaćanjem;	Potpuno usklađeno		
14. „kibernapad“ znači zlonamjerna IKT incident uzrokovan pokušajem bilo kojeg aktera prijetnje da uništi, izloži, izmijeni, onemogući, ukrade ili neovlašteno koristi imovinu ili joj neovlašteno pristupi;	Član 8, stav 1, tačka 13 13) sajber napad je zlonamjerna IKT incident izazvan pokušajem bilo kojeg aktera da uništi, razotkrije, izmijeni, onemogući, ukrade imovinu, stekne neovlašćeni pristup imovini ili je neovlašćeno koristi;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 14 14) saznanja o prijetnjama su informacije koje su agregirane, prilagođene, analizirane, protumačene ili dopunjene radi utvrđivanja potrebe donošenja odluka i omogućavanja adekvatnog i dovoljnog razumijevanja u cilju ublažavanja posljedica IKT incidenta ili sajber prijetnje, uključujući informacije o tehničkim detaljima sajber napada, licima odgovornim za napad, njihovom načinu djelovanja i motivima;	Potpuno usklađeno		
16. „ranjivost“ znači slabost, osjetljivost ili nedostatak neke imovine, sustava, procesa ili kontrole koji se može iskoristiti;	Član 8, stav 1, tačka 15 15) ranjivost je slabost, podložnost ili nedostatak resursa, sistema, procesa ili kontrole koju sajber prijetnja može iskoristiti;	Potpuno usklađeno		
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“);	Član 8, stav 1, tačka 16 16) penetraciono testiranje vođeno prijetnjama (TLPT) je kontrolisano, prilagođeno testiranje kritičnih produkcijskih sistema koje finansijski subjekt koristi, zasnovano na saznanjima o prijetnjama, odnosno testiranje crvenog tima, koje se sprovodi u skladu sa okvirom koji oponaša taktike, tehnike i postupke stvarnih zlonamjernih aktera za koje se vjeruje da predstavljaju realnu sajber prijetnju;	Potpuno usklađeno		
18. „IKT rizik povezan s trećim stranama“ znači IKT rizik koji može nastati za finansijski subjekt u vezi s upotrebom IKT usluga koje pružaju treće strane pružatelji IKT usluga ili njihovi podugovaratelji, među ostalim i putem aranžmana za eksternalizaciju;	Član 8, stav 1, tačka 19 19) IKT rizik povezan sa trećim stranama je IKT rizik kojem finansijski subjekt može biti izložen zbog korišćenja IKT usluga koje pružaju treće strane ili njihovi podizvođači, uključujući i na osnovu ugovora o eksternalizaciji;	Potpuno usklađeno		
19. „treća strana pružatelj IKT usluga“ znači poduzetnik koji pruža IKT usluge;	Član 8, stav 1, tačka 20	Potpuno usklađeno		

	20) treća strana koja pruža IKT usluge je pravno ili fizičko lice koje 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;	Član 8, stav 1, tačka 21 21) grupni pružatelj IKT usluga je pravno lice koje je dio financijske grupe i koje pruža IKT usluge pretežno financijskim subjektima koji su dio iste grupe ili financijskim subjektima koji pripadaju istom institucionalnom sustavu zaštite, uključujući i njihova matična pravna lica, zavisna pravna lica, filijale i druge subjekte koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom;	Potpuno usklađeno		
21. „IKT usluge” znači digitalne i podatkovne usluge koje se putem IKT sustava 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;	Član 8, stav 1, tačka 22 22) IKT usluge su digitalne usluge i usluge vezane za podatke koje se pomoću IKT sistema, kontinuirano pružaju jednom ili više internih ili eksternih korisnika, uključujući usluge iznajmljivanja IKT opreme („hardver kao usluga”) i hardverske usluge koje uključuju pružanje tehničke podrške od strane pružatelja hardvera putem ažuriranja softvera ili firmvera, osim tradicionalnih analognih telefonskih usluga;	Potpuno usklađeno		
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 narušilo sposobnost financijskog subjekta da kontinuirano ispunjava uvjete i obveze iz svojeg odobrenja za rad ili druge obveze na temelju primjenjivog prava o financijskim uslugama;	Član 8, stav 1, tačka 23 23) kritična ili važna funkcija je funkcija čiji bi poremećaj značajno narušio financijske rezultate financijskog subjekta, pouzdanost, kontinuitet njegovih usluga i aktivnosti, ili funkcija čiji bi prekidi, neispravno ili neuspješno izvršavanje značajno narušilo sposobnost tog subjekta da kontinuirano ispunjava uslove i obaveze utvrđene dozvolom za rad ili druge obaveze u skladu sa propisima kojima se uređuje pružanje financijskih usluga;	Potpuno usklađeno		
23. „ključna treća strana pružatelj IKT usluga” znači treća strana pružatelj IKT usluga imenovana kao ključna u skladu s člankom 31.;	Član 8, stav 1, tačka 24 24) kritična treća strana koja pruža IKT usluge je treća strana koja pruža IKT usluge i koja je određena kao kritična u skladu sa članom 31. Regulative (EU) br. 2022/2554;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 25 25) treća strana koja pruža IKT usluge sa sjedištem u trećoj zemlji je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa financijskim subjektom za pružanje IKT usluga;	Potpuno usklađeno		

25. „društvo kći“ znači poduzeće kći u smislu članka 2. točke 10. i članka 22. Direktive 2013/34/EU;	Član 8, stav 1, tačka 28 28) zavisno pravno lice je pravno lice koje je pod kontrolom matičnog pravnog lica, uključujući i bilo koje pravno lice koje je pod kontrolom krajnjeg matičnog pravnog lica;	Potpuno usklađeno		
26. „grupa“ znači grupa kako je definirana u članku 2. točki 11. Direktive 2013/34/EU;	Član 8, stav 1, tačka 29 29) grupa je matično pravno lice i sva njegova zavisna pravna lica;	Potpuno usklađeno		
27. „matično društvo“ znači matično poduzeće u smislu članka 2. točke 9. i članka 22. Direktive 2013/34/EU;	Član 8, stav 1, tačka 30 30) matično pravno lice ima značenje utvrđeno zakonom kojim se uređuje računovodstvo;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 31 31) IKT podizvođač sa sjedištem u trećoj zemlji je IKT podizvođač koji je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa trećom stranom koja pruža IKT usluge, bez obzira na sjedište treće strane koja pruža IKT usluge;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 32 32) rizik IKT koncentracije je izloženost prema jednoj ili više povezanih trećih strana koje pružaju IKT usluge, kojom se stvara zavisnost od tih trećih strana na način da njihova nedostupnost, propast ili druga vrsta nedostatka može potencijalno da ugrozi sposobnost financijskog subjekta da obavlja kritične ili važne funkcije, ili prouzrokuje druge vrste negativnih uticaja, uključujući značajne gubitke, ili ugrozi financijsku stabilnost tržišta kao cjeline;	Potpuno usklađeno		
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 kriptovaluta ili ekvivalentne osobe koje u praksi upravljaju subjektom ili imaju ključne funkcije u skladu s relevantnim pravom Unije ili nacionalnim pravom;	Član 8, stav 1, tačka 33 33) organ upravljanja je: - jedan ili više organa financijskog subjekta, koji su u skladu sa propisima ovlašćeni da utvrđuju strategiju, ciljeve i opšte usmjerenje tog financijskog subjekta i koji vrše nadzor i prate odlučivanje u vezi sa upravljanjem i uključuje lica koja stvarno upravljaju poslovanjem tog financijskog subjekta; ili - lica koja imaju ovlaštenja jednaka ovlaštenjima iz alineje 1 ove tačke i koja, u skladu sa propisima, vode poslove financijskog subjekta ili imaju ključne funkcije;	Potpuno usklađeno		

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);	Član 8, stav 1, tačka 34 34) kreditna institucija ima značenje utvrđeno zakonom kojim se uređuje poslovanje kreditnih institucija;	Potpuno usklađeno		
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;	Nema odgovarajuće odredbe	Potpuno usklađeno	U tekstu se direktno koristi termin „Razvojna banka Crne Gore“	
33. „investicijsko društvo“ znači investicijsko društvo kako je definirano u članku 4. stavku 1. točki 1. Direktive 2014/65/EU;	Član 8, stav 1, tačka 38 38) investiciono društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
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);	Član 8, stav 1, tačka 39 39) malo i nepovezano investiciono društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
5. „institucija za platni promet“ znači institucija za platni promet kako je definirana u članku 4. točki 4. Direktive (EU) 2015/2366;	Član 8, stav 1, tačka 35 35) platna institucija sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;	Potpuno usklađeno		
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;	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti. U Zakonu o platnom prometu nije iskorištena opcija/diskrecija iz člana 32 Direktive 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;	Član 8, stav 1, tačka 36 36) registrovani pružalac usluge informacija o računu sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;	Potpuno usklađeno		
38. „institucija za elektronički novac“ znači institucija za elektronički novac kako je definirana u članku 2. točki 1. Direktive 2009/110/EZ;	Član 8, stav 1, tačka 37 37) institucija za elektronski novac sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;	Potpuno usklađeno		

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;	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti. U Zakonu o platnom prometu nije iskorištena opcija/diskrecija iz člana 9 Direktive 2009/110/EC	
40. „središnja druga ugovorna strana” znači središnja druga ugovorna strana kako je definirana u članku 2. točki 1. Uredbe (EU) br. 648/2012;	Član 8, stav 1, tačka 41 41) centralna druga ugovorna strana ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
41. „trgovinski repozitorij” znači trgovinski repozitorij kako je definiran u članku 2. točki 2. Uredbe (EU) br. 648/2012;	Član 8, stav 1, tačka 43 43) trgovinski repozitorij ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
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;	Član 8, stav 1, tačka 40 40) centralno klirinško depozitarno društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
43. „mjesto trgovanja” znači mjesto trgovanja kako je definirano u članku 4. stavku 1. točki 24. Direktive 2014/65/EU;	Član 8, stav 1, tačka 42 42) mjesto trgovanja ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		
44. „upravitelj alternativnih investicijskih fondova” znači upravitelj alternativnih investicijskih fondova kako je definiran u članku 4. stavku 1. točki (b) Direktive 2011/61/EU;	Član 8, stav 1, tačka 44 44) društvo za upravljanje alternativnim investicionim fondom ima značenje utvrđeno zakonom kojim se uređuje poslovanje alternativnih fondova;	Potpuno usklađeno		
45. „društvo za upravljanje” znači društvo za upravljanje kako je definirano u članku 2. stavku 1. točki (b) Direktive 2009/65/EZ;	Član 8, stav 1, tačka 45 45) društvo za upravljanje otvorenim investicionim fondom sa javnom ponudom ima značenje utvrđeno zakonom kojim se uređuje poslovanje otvorenih investicionih fondova sa javnom ponudom;	Potpuno usklađeno		
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.;	Član 8, stav 1, tačka 48 48) pružalac usluga dostave podataka ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;	Potpuno usklađeno		

47. „društvo za osiguranje“ znači društvo za osiguranje kako je definirano u članku 13. točki 1. Direktive 2009/138/EZ;	Član 8, stav 1, tačka 50 50) društvo za osiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;	Potpuno usklađeno		
48. „društvo za reosiguranje“ znači društvo za reosiguranje kako je definirano u članku 13. točki 4. Direktive 2009/138/EZ;	Član 8, stav 1, tačka 51 51) društvo za reosiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;	Potpuno usklađeno		
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);	Član 8, stav 1, tačka 54 54) društvo za posredovanje u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;	Potpuno usklađeno		
50. „sporedni posrednik u osiguranju“ znači sporedni posrednik u osiguranju kako je definiran u članku 2. stavku 1. točki 4. Direktive (EU) 2016/97;	Član 8, stav 1, tačka 55 55) sporedni posrednik u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;	Potpuno usklađeno		
51. „posrednik u reosiguranju“ znači posrednik u reosiguranju kako je definiran u članku 2. stavku 1. točki 5. Direktive (EU) 2016/97;	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti	
52. „institucija za strukovno mirovinsko osiguranje“ znači institucija za strukovno mirovinsko osiguranje kako je definirana u članku 6. točki 1. Direktive (EU) 2016/2341;	Član 8, stav 1, tačka 46 46) institucija za profesionalnu penzionu štednju ima značenje utvrđeno zakonom koji uređuje dobrovoljne penzione fondove;	Potpuno usklađeno		
53. „mala institucija za strukovno mirovinsko osiguranje“ znači institucija za strukovno mirovinsko osiguranje koja upravlja mirovinskim programima koji ukupno imaju manje od 100 članova;	Član 8, stav 1, tačka 47 47) mala institucija za profesionalnu penzionu štednju je institucija za profesionalnu penzionu štednju koja upravlja penzionim programima koji ukupno imaju manje od 100 članova;	Potpuno usklađeno		
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;	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti	
55. „pružatelj usluga povezanih s kriptovalutama“ znači pružatelj usluga povezanih s kriptovalutama kako je definiran u relevantnoj odredbi Uredbe o tržištima kriptovalutama;	Član 8, stav 1, tačka 61 61) pružatelj usluga povezanih s kriptovalutama ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;	Potpuno usklađeno		
56. „izdavalac tokena vezanih uz imovinu“ znači izdavalac tokena vezanih uz imovinu kako je definiran u relevantnoj odredbi Uredbe o tržištima kriptovalutama;	Član 8, stav 1, tačka 62 62) izdavalac tokena vezanih uz imovinu ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;	Potpuno usklađeno		
57. „administrator ključnih referentnih vrijednosti“ znači administrator „ključnih referentnih vrijednosti“ kako su definirane u članku 3. točki 25. Uredbe (EU) 2016/1011;	Član 8, stav 1, tačka 49 49) administrator ključnih referentnih vrijednosti ima značenje utvrđeno zakonom kojim se uređuju referentne vrijednosti;	Potpuno usklađeno		

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);	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti	
59. „sekuritizacijski repozitorij“ znači sekuritizacijski repozitorij kako je definiran u članku 2. točki 23. Uredbe (EU) 2017/2402 Europskog parlamenta i Vijeća (36);	Nema odgovarajuće odredbe	Neprenosivo	U Crnoj Gori ne postoje ovi subjekti	
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;	Klasifikacija financijskih subjekata prema veličini Član 6, stav 1, tačka 1 (1) U smislu ovog zakona, u zavisnosti od prosječnog broja zaposlenih, ukupnog prihoda na godišnjem nivou i ukupne aktive, financijski subjekti se klasifikuju kao: 1) mikro financijski subjekti, ako: - imaju prosječan broj zaposlenih u poslovnoj godini manji od deset; - i - ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu do 2.000.000,00 eura; Član 6, stav 6 (6) Izuzetno od stava 1 tačka 1 ovog člana, financijski subjekt koji je mjesto trgovanja, centralna druga ugovorna strana, trgovinski repozitorij ili centralno klirinško depozitarno društvo i ispunjava uslove da bude klasifikovan kao mikro financijski subjekt, klasifikuje se kao ostali financijski subjekt.	Potpuno usklađeno		
61. „glavno nadzorno tijelo“ znači europsko nadzorno tijelo imenovano u skladu s člankom 31. stavkom 1. točkom (b) ove Uredbe;	Ključne ugovorne odredbe Član 38 stav 4, tačka 5, alineja 4 (4) Ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije mora, pored elemenata iz stava 3 ovog člana, da sadrži i: 5) pravo kontinuiranog praćenja učinka treće strane koja pruža IKT usluge, što obuhvata: - obavezu treće strane koja pruža IKT usluge da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, tokom nadzora koji sprovodi taj organ; Saradnja sa organima Evropske unije i organima trećih država Član 45, stav 6	Potpuno usklađeno	U relevantnim odredbama sa odloženom primjenom (Član 38, stav 4, tačka 5, alineja 4 i Član 45, stav 6) se direktno koristi termin „glavni nadzorni organ, koji je određen u skladu sa članom 31 stav 1 tačka	

	(6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlašćenja glavnog nadzornog organa u pogledu sprovođenja nadzora.		b) Regulative (EU) br. 2022/2554"	
62. „Zajednički odbor“ znači odbor iz članka 54. uredbi (EU) br. 1093/2010, (EU) br. 1094/2010 i (EU) br. 1095/2010;	Nema odgovarajuće odredbe	Neprenosivo		
63. „malo poduzeće“ znači finansijski 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;	Član 6, stav 1, tačka 2 (1) U smislu ovog zakona, u zavisnosti od prosječnog broja zaposlenih, ukupnog prihoda na godišnjem nivou i ukupne aktive, finansijski subjekti se klasifikuju kao: 2) mali finansijski subjekti, ako: - imaju prosječan broj zaposlenih u poslovnoj godini u rasponu od deset do 49; i - ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu u rasponu od 2.000.000,01 eura do 10.000.000,00 eura;	Potpuno usklađeno		
64. „srednje poduzeće“ znači finansijski 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;	Član 6, stav 1, tačka 3 (1) U smislu ovog zakona, u zavisnosti od prosječnog broja zaposlenih, ukupnog prihoda na godišnjem nivou i ukupne aktive, finansijski subjekti se klasifikuju kao: 3) srednji finansijski subjekti, ako: - imaju prosječan broj zaposlenih u poslovnoj godini manji od 250; i - ostvaruju ukupan prihod na godišnjem nivou do 50.000.000,00 eura i/ili ukupnu aktivu do 43.000.000,00 eura;	Potpuno usklađeno		
65. „tijelo javne vlasti“ znači svako državno tijelo ili drugo tijelo javne uprave, uključujući nacionalne središnje banke.	Član 8, stav 1, tačka 63 63) javni organ je svaki organ državne uprave, drugi državni organ ili organ sa javnim ovlašćenjima, uključujući Centralnu banku Crne Gore;	Potpuno usklađeno		

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.	Princip proporcionalnosti Član 5, stav 1 (1) Financijski subjekt je dužan da primjenjuje odredbe ovog zakona srazmjerno svojoj veličini, ukupnom rizičnom profilu, prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, na način utvrđen ovim zakonom.	Potpuno usklađeno		
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.	Princip proporcionalnosti Član 5, stav 1 (1) Financijski subjekt je dužan da primjenjuje odredbe ovog zakona srazmjerno svojoj veličini, ukupnom rizičnom profilu, prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, na način utvrđen ovim zakonom.	Potpuno usklađeno		
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.	Član 5, stav 2 (2) Nadležni organ razmatra primjenu principa proporcionalnosti iz stava 1 ovog člana prilikom procjene konzistentnosti sistema financijskog subjekta za upravljanje IKT rizicima, uzimajući u obzir izvještaje koji se dostavljaju na zahtjev nadležnog organa u skladu sa članom 11 stav 3 ovog zakona, odnosno članom 21 ovog zakona.	Potpuno usklađeno		
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.	II. UPRAVLJANJE IKT RIZICIMA Korporativno upravljanje i organizacija Član 9, stav 2 (2) Financijski subjekt dužan je da uspostavi sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima, u skladu sa članom 10 st. 5 i 6 ovog zakona, radi postizanja visokog nivoa digitalne operativne otpornosti.	Potpuno usklađeno		
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;	Korporativno upravljanje i organizacija Član 9, st. 1 i 3 (1) Organ upravljanja financijskog subjekta dužan je da obezbijedi da financijski subjekt postupa u skladu sa odredbama ovog zakona. (3) Organ upravljanja financijskog subjekta dužan je da utvrdi, odobri i nadzire sva pravila, postupke, procese, mehanizme, mjere i resurse povezane sa sistemom upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona i da obezbijedi njihovu primjenu, i u tom cilju naročito da:	Potpuno usklađeno		

(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 osigurala 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:	1) uspostavlja politike sa ciljem održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka; 2) jasno utvrđuje ovlašćenja, zaduženja i odgovornosti za obavljanje svih poslova povezanih sa IKT i uspostavlja odgovarajuće mehanizme upravljanja kako bi se, na svim organizacionim nivoima, obezbijedila efikasna i blagovremena komunikacija, saradnja i koordinacija u vezi sa obavljanjem tih poslova; 3) utvrđuje strategiju digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona, uključujući i odgovarajući nivo tolerancije finansijskog subjekta prema IKT riziku iz člana 12 stav 2 tačka 2 ovog zakona; 4) usvaja i periodično preispituje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona i planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i nadzire njihovu primjenu; 5) odobrava i periodično preispituje planove interne revizije u IKT oblasti, njihove značajne izmjene i da redovno razmatra rezultate revizija u IKT oblasti; 6) donosi i periodično preispituje odgovarajući plan raspodjele finansijskih sredstava za ispunjavanje svih potreba finansijskog subjekta u pogledu digitalne operativne otpornosti, uključujući i sprovođenje relevantnih programa za podizanje svijesti o IKT bezbjednosti i obuka o digitalnoj operativnoj otpornosti iz člana 19 stav 10 ovog zakona i sticanje znanja i vještina u IKT oblasti za sve zaposlene; 7) usvaja i periodično preispituje politiku o korišćenju IKT usluga koje pružaju treće strane koje pružaju IKT usluge; 8) na nivou cijele organizacije uspostavlja mehanizme izvještavanja za blagovremeno i adekvatno informisanje u vezi sa: - zaključenim ugovorima sa trećim stranama koje pružaju IKT usluge; - svim planiranim značajnim promjenama u vezi sa trećim stranama koje pružaju IKT usluge;	
---	---	--

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.	- potencijalnim uticajem promjena iz alineje 2 ove tačke na kritične ili važne funkcije, uključujući rezime analize rizika za procjenu uticaja tih promjena; - IKT incidentima, a najmanje o značajnim IKT incidentima i njihovom uticaju, kao i o odgovoru, oporavku i korektivnim mjerama. Član 17 stav 2 (2) IKT politika kontinuiteta poslovanja iz stava 1 ovog člana predstavlja sastavni dio opšte politike kontinuiteta poslovanja finansijskog subjekta, a može se usvojiti u formi zasebnog, namjenskog akta.			
3. Finansijski 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.	Član 9, stav 4 (4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi organizacioni dio odgovoran za praćenje realizacije ugovora zaključenih sa trećim stranama koje pružaju IKT usluge, ili da imenuje člana višeg rukovodstva koji će biti odgovoran za nadzor izloženosti prema povezanom riziku i pripadajuće dokumentacije.	Potpuno usklađeno		
4. Članovi upravljačkog tijela finansijskog subjekta aktivno osvježavaju znanje i vještine koji su im dostatni kako bi mogli razumjeti i procijeniti IKT rizik i njegov učinak na poslovanje finansijskog subjekta, među ostalim i tako da redovito pohađaju posebno osposobljavanje, razmjerno IKT riziku kojima se upravlja.	Član 9, stav 5 (5) Članovi organa upravljanja dužni su da aktivno unapređuju znanje i vještine potrebne za razumijevanje i procjenu IKT rizika i njegovog uticaja na poslovanje finansijskog subjekta, uključujući i kroz redovne posebne obuke, srazmjerno prirodi rizika kojim se upravlja.	Potpuno usklađeno		
Odjeljak II. Članak 6. Okvir za upravljanje IKT rizicima 1. Finansijski 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.	Sistem upravljanja IKT rizicima Član 10, stav 1 (1) Finansijski subjekt je dužan da uspostavi pouzdan, sveobuhvatan i dobro dokumentovan sistem upravljanja IKT rizicima, kao dio opšteg sistema upravljanja rizicima, kojim se omogućava brzo, efikasno i sveobuhvatno tretiranje IKT rizika i obezbjeđuje visok nivo digitalne operativne otpornosti.	Potpuno usklađeno		
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	Član 10, stav 2 (2) Sistem upravljanja IKT rizicima iz stava 1 ovog člana, najmanje obuhvata strategije, politike, procedure, IKT protokole i alate	Potpuno usklađeno		

imovine, što uključuje računalni softver, hardver i poslužitelje, te za zaštitu svih relevantnih fizičkih komponenta 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 rizika, među ostalim i od oštećenja te neovlaštenog pristupa ili upotrebe.	potrebne za pravilnu i adekvatnu zaštitu cjelokupne informacione imovine i IKT imovine, uključujući softver, servere i ostali hardver i zaštitu svih relevantnih fizičkih komponenti i infrastrukture, kao što su prostori, računalni centri i posebna osjetljiva područja, kako bi se obezbijedilo da je sva informaciona imovina i IKT imovina adekvatno zaštićena od rizika, uključujući oštećenja, neovlašten pristup ili korišćenje.			
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.	Član 10, stav 3 (3) Financijski subjekt je dužan da, u skladu sa sistemom upravljanja IKT rizicima, svede na najmanju moguću mjeru uticaj IKT rizika, primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata iz stava 2 ovog člana. Član 10, stav 4 (4) Financijski subjekt je dužan da nadležnom organu, na njegov zahtjev, dostavi potpune i ažurne informacije o IKT rizicima i sistemu upravljanja IKT rizicima iz stava 1 ovog člana.	Potpuno usklađeno		
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.	Član 10, st. 5 i 6 (5) Financijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odgovornost za upravljanje i nadzor nad IKT rizikom dodijeli kontrolnoj funkciji i da obezbijedi odgovarajući nivo njene nezavisnosti, na način da se izbjegava sukob interesa. (6) Financijski subjekt je dužan da obezbijedi međusobnu nezavisnost i razdvajanje poslova u kojima IKT rizik nastaje, poslova kontrolnih funkcija i poslova interne revizije, u skladu sa modelom tri linije odbrane ili internim modelom za upravljanje i kontrolu rizika.	Potpuno usklađeno		
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 operative 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.	Unaprjeđivanje i revizija sistema upravljanja IKT rizicima Član 11, st. 1 do 3 (1) Financijski subjekt je dužan da kontinuirano unaprjeđuje sistem upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona na osnovu iskustava stečenih kroz njegovu praktičnu primjenu i praćenje, kao i da taj sistem preispituje i ažurira: 1) najmanje jednom godišnje; 2) u slučaju značajnog IKT incidenta; 3) na zahtjev nadležnog organa;	Potpuno usklađeno		

	4) u skladu sa rezultatima testiranja digitalne operativne otpornosti; 5) u skladu sa zaključcima revizije. (2) Izuzetno od stava 1 tačka 1 ovog člana, finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da preispituje i ažurira sistem upravljanja IKT rizicima iz stava 1 ovog člana periodično. (3) Finansijski subjekt je dužan da izvještaj o preispitivanju i ažuriranju iz st. 1 i 2 ovog člana dostavi nadležnom organu, na njegov zahtjev.			
6. Okvir za upravljanje IKT rizicima finansijskih subjekata koji nisu mikropoduzeća podliježe redovitoj unutarnjoj reviziji, koju revizori provode u skladu s planom revizije finansijskog 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 finansijskog subjekta.	Član 11, st. 4 i 5 (4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi redovne interne revizije sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, u skladu sa planom revizije, od strane nezavisnih revizora koji posjeduju znanje, vještine i iskustvo u oblasti IKT rizika. (5) Učestalost i predmet revizija iz stava 4 ovog člana moraju biti srazmjerni IKT riziku finansijskog subjekta.	Potpuno usklađeno		
7. Finansijski subjekti na temelju zaključaka unutarnjeg revizijskog pregleda uspostavljaju formalni proces daljnje postupanja, uključujući pravila za pravodobnu provjeru i ispravljanje ključnih nalaza revizije u području IKT-a.	Član 11, stav 6 (6) Finansijski subjekt je dužan da uspostavi formalan proces koji omogućava blagovremeno otklanjanje ključnih nepravilnosti i nedostataka utvrđenih revizijom iz stava 4 ovog člana, kao i adekvatnu provjeru i praćenje tog postupka.	Potpuno usklađeno		
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 slijedeći način: (a) objašnjava se kako se okvirom za upravljanje IKT rizicima podupiru poslovna strategija i ciljevi finansijskog subjekta; (b) utvrđuje se razina tolerancije na IKT rizik, u skladu sa sklonošću finansijskog subjekta preuzimanju rizika, te se analizira učinak tolerancije za poremećaje u radu IKT-a;	Strategija digitalne operativne otpornosti Član 12, st. 1 i 2 (1) Finansijski subjekt je dužan da u strategiji digitalne operativne otpornosti, koja predstavlja sastavni dio sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, utvrdi način primjene tog sistema. (2) Strategija iz stava 1 ovog člana mora da obuhvati opšte kriterijume i metode za tretiranje IKT rizika i postizanje konkretnih IKT ciljeva, a najmanje mora da: 1) opisuje i objašnjava kako sistem za upravljanje IKT rizicima podržava poslovnu strategiju i ciljeve finansijskog subjekta;	Potpuno usklađeno		

(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.	2) utvrđuje nivo tolerancije prema IKT riziku, u skladu sa sklonošću finansijskog subjekta ka preuzimanju rizika, i sadrži analizu prihvatljivog uticaja IKT poremećaja; 3) definiše jasne ciljeve u oblasti informacione bezbjednosti, uključujući ključne indikatore uspješnosti i ključne metrike rizika; 4) opisuje i objašnjava referentnu, odnosno ciljanu IKT arhitekturu i sve promjene potrebne za postizanje konkretnih poslovnih ciljeva; 5) okvirno navodi različite mehanizme uspostavljene radi otkrivanja IKT incidenata, sprečavanja njihovog uticaja i obezbjeđivanja zaštite od tog uticaja; 6) jasno prikazuje postojeće stanje digitalne operativne otpornosti, na osnovu informacija o broju prijavljenih značajnih IKT incidenata i efikasnosti preventivnih mjera; 7) predviđa sprovođenje testiranja digitalne operativne otpornosti, u skladu sa odredbama čl. 27 do 32 ovog zakona; 8) utvrđuje strategiju komunikacije u slučaju IKT incidenata o kojima se informacije saopštavaju u skladu sa članom 20 ovog zakona.			
9. U kontekstu strategije za digitalnu operativnu otpornost iz stavka 8. finansijski 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.	Član 12, stav 3 (3) Finansijski subjekt može, da utvrdi sveobuhvatnu strategiju IKT nabavke od više dobavljača, na nivou grupe ili subjekta, kojom se identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge i obrazlažu razlozi za diverzifikaciju dobavljača.	Potpuno usklađeno		
10. Finansijski subjekti mogu, u skladu sa sektorskim pravom Unije i nacionalnim sektorskim pravom, eksternalizirati zadatke provjeravanja usklađenosti sa zahtjevima u pogledu upravljanja IKT rizicima društvima unutar grupe ili vanjskim društvima. U slučaju takve eksternalizacije finansijski subjekt ostaje u potpunosti odgovoran za provjeru usklađenosti sa zahtjevima u pogledu upravljanja IKT rizicima.	Član 12, st. 4 i 5 (4) Finansijski subjekt može, u skladu sa zakonom, da povjeri obavljanje poslova provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima subjektima unutar grupe ili drugim subjektima. (5) U slučaju iz stava 4 ovog člana, finansijski subjekt zadržava odgovornost za usklađenost sa zahtjevima za upravljanje IKT rizicima, kao i za provjeru te usklađenosti.	Potpuno usklađeno		
Članak 7. IKT sustavi, protokoli i alati	IKT sistemi, protokoli i alati Član 13	Potpuno usklađeno		

Kako bi odgovorili na IKT rizik i upravljali njime, finansijski subjekti upotrebljavaju i održavaju ažuriranim IKT sustave, protokole i alate koji su: (a) primjereni razmjeru operacija koje podupiru poslovanje tih finansijskih 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 nalogima, 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.	Finansijski subjekt je dužan da, radi tretiranja i upravljanja IKT rizikom, koristi i održava ažurnim IKT sisteme, protokole i alate koji moraju biti: 1) primjereni za obim operacija koje podržavaju njegovo poslovanje, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona; 2) pouzdani; 3) dovoljnog kapaciteta za tačnu obradu podataka neophodnih za obavljanje aktivnosti i blagovremeno pružanje usluga, kao i kapacitet za obradu u uslovima najvećeg opterećenja u pogledu obima naloga, poruka ili transakcija, u skladu sa potrebama, uključujući i u slučaju uvođenja nove tehnologije; 4) tehnološki otporni kako bi mogli na adekvatan način odgovoriti na dodatne potrebe za obradom informacija koje nastaju usljed poremećaja na tržištu ili u drugim nepovoljnim situacijama.			
Članak 8. Utvrđivanje 1. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. finansijski 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. Finansijski subjekti prema potrebi, a najmanje jedanput godišnje, preispituju primjerenost te klasifikacije i sve relevantne dokumentacije.	Identifikacija i procjena IKT rizika, usluga, sistema i imovine Član 14, st. 1 i 2 (1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, identifikuje, klasifikuje i adekvatno dokumentuje sve poslovne funkcije podržane IKT-om, zaduženja i odgovornosti, informacionu imovinu i IKT imovinu koja podržava te funkcije, kao i njihove uloge i međuzavisnosti u pogledu IKT rizika. (2) Finansijski subjekt je dužan da, po potrebi, a najmanje jednom godišnje, preispituje adekvatnost klasifikacije iz stava 1 ovog člana i cjelokupne pripadajuće dokumentacije.	Potpuno usklađeno		
2. Finansijski subjekti kontinuirano utvrđuju sve izvore IKT rizika, osobito izloženost riziku drugih finansijskih subjekata i od drugih finansijskih 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. Finansijski subjekti redovito, a najmanje jedanput godišnje, preispituju scenarije rizika koji utječu na njih.	Član 14, st. 3 i 4 (3) Finansijski subjekt je dužan da kontinuirano: 1) identifikuje sve izvore IKT rizika, a naročito izloženosti riziku prema drugim finansijskim subjektima i od drugih finansijskih subjekata; 2) procjenjuje sajber prijetnje i IKT ranjivosti koje se odnose na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu.	Potpuno usklađeno		

	(4) Finansijski subjekt je dužan da redovno, a najmanje jednom godišnje, razmatra scenarije rizika koji mogu da utiču na funkcije i imovinu iz stava 3 tačka 2 ovog člana.			
3. Finansijski 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.	Član 14, stav 5 (5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da sprovede procjenu rizika u slučaju svake značajne promjene u: 1) infrastrukturi mrežnih i informacionih sistema; 2) procesima ili procedurama koje utiču na njegove poslovne funkcije podržane IKT-om, informacionu imovinu ili IKT imovinu.	Potpuno usklađeno		
4. Finansijski 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. Finansijski subjekti mapiraju konfiguraciju informacijske imovine i IKT imovine te veze među različitim informacijskom imovinom i IKT imovinom i njihove međuzavisnosti.	Član 14, st. 6 i 7 (6) Finansijski subjekt je dužan da identifikuje svu informacionu imovinu i IKT imovinu, uključujući mrežne resurse, hardversku opremu i imovinu na udaljenim lokacijama, i da posebno evidentira informacionu imovinu i IKT imovinu koja se smatra kritičnom. (7) Finansijski subjekt je dužan da dokumentuje konfiguraciju informacione imovine i IKT imovine i informacije o povezanosti i međuzavisnosti između različite informacione i IKT imovine.	Potpuno usklađeno		
5. Finansijski 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.	Član 14, stav 8 (8) Finansijski subjekt je dužan da identifikuje i dokumentuje sve procese koji zavise od trećih strana koje pružaju IKT usluge, kao i da identifikuje međusobne povezanosti sa trećim stranama koje pružaju IKT usluge kojima se podržavaju kritične ili važne funkcije.	Potpuno usklađeno		
6. Za potrebe stavaka 1., 4. i 5. finansijski subjekti vode relevantne evidencije, koje ažuriraju redovito i svaki put kad dođe do značajnih promjena iz stavka 3.	Član 14, stav 9 (9) Finansijski subjekt je dužan da, radi postupanja u skladu sa st. 1, 6, 7 i 8 ovog člana, vodi odgovarajuće registre, koje mora da ažurira redovno i u slučaju svake značajne promjene iz stava 5 ovog člana.	Potpuno usklađeno		
7. Finansijski 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.	Član 14, stav 10 (10) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da redovno, a najmanje jednom godišnje, sprovodi procjenu IKT rizika za sve zastarjele IKT sisteme, kao i vanredno prije i nakon povezivanja tehnologija, aplikacija ili sistema.	Potpuno usklađeno		
Članak 9. Zaštita i sprečavanje	Zaštita IKT sistema i sprečavanje IKT incidenata Član 15, stav 1	Potpuno usklađeno		

1. Za potrebe primjerene zaštite IKT sustava i u cilju organiziranja mjera odgovora, financijski subjekti kontinuirano prate i kontroliraju sigurnost i funkcioniranje IKT sustava i alata te učinak IKT rizika na IKT sustave svode na najmanju moguću mjeru uvođenjem odgovarajućih alata, politika i postupaka za sigurnost IKT-a.	(1) Radi adekvatne zaštite IKT sistema i u cilju organiziranja mjera odgovora, financijski subjekt dužan je da kontinuirano prati i kontrolira bezbjednost i funkcionisanje IKT sistema i alata, kao i da na najmanju moguću mjeru svede uticaj IKT rizika na IKT sisteme, primjenom odgovarajućih IKT bezbjednosnih alata, politika i procedura.			
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.	Član 15, stav 2 (2) Financijski subjekt je dužan da osmisli, kreira i/ili nabavi i primijeni politike, procedure, protokole i alate za IKT bezbjednost u cilju obezbjeđivanja otpornosti, kontinuiteta i dostupnosti IKT sistema, a naročito onih koji podržavaju kritične ili važne funkcije, i u cilju održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, bez obzira da li su u stanju mirovanja, upotrebi ili prenosu.	Potpuno usklađeno		
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, kršenje povjerljivosti i gubitak podataka; (d) osigurava se zaštita podataka od rizika koji proizlaze iz upravljanja podacima, među ostalim i iz loše administracije, rizika povezanih s obradom i ljudske pogreške.	Član 15, stav 3 (3) Radi ostvarivanja ciljeva iz stava 2 ovog člana, financijski subjekt je dužan da koristi IKT rješenja i procese koji su primjereni, u smislu člana 5 ovog zakona i kojima se: 1) omogućava bezbjednost sredstava i metoda za prenos podataka; 2) na najmanju moguću mjeru svodi rizik od oštećenja ili gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje; 3) sprečava nedostupnost i gubitak podataka, narušavanje autentičnosti, integriteta i povjerljivosti podataka; 4) obezbjeđuje zaštitu podataka od rizika koji proizlaze iz upravljanja podacima, uključujući propuste u administraciji, rizike povezane sa obradom i ljudske greške.	Potpuno usklađeno		
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;	Član 15, st. 4 do 7 (4) Financijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima: 1) razvije i usvoji politiku informacione bezbjednosti kojom se utvrđuju pravila za zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, informacione imovine i IKT imovine,	Potpuno usklađeno		

(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 kibernetičkog napada; (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 finansijskom 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) finansijski 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 finansijskih procesa. Za potrebe prvog podstavka točke (e) proces upravljanja promjenama IKT-a odobravaju odgovarajuće razine rukovodstva te on mora sadržavati posebne protokole.	uključujući podatke i imovinu njegovih klijenata, kada je to primjenljivo; 2) primjenom pristupa zasnovanog na procjeni rizika, uspostavi pouzdanu strukturu za upravljanje mrežom i infrastrukturom, korišćenjem odgovarajućih tehnika, metoda i protokola; 3) utvrdi i primjenjuje politike kojima se odobrava fizički i logički pristup informacionoj imovini i IKT imovini do nivoa koji je neophodan za obavljanje opravdanih i odobrenih poslova i aktivnosti, i u tu svrhu primjenjuje skup pravila, postupaka i kontrola za adekvatno upravljanje pravima pristupa i kontrolu pristupa; 4) utvrdi i primjenjuje politike i protokole za korišćenje pouzdanih mehanizama provjere autentičnosti, zasnovanih na relevantnim standardima i specijalizovanim sistemima kontrole, kao i mjere za zaštitu kriptografskih ključeva za šifrovanje podataka; 5) utvrdi i primjenjuje politike, procedure i kontrole za upravljanje IKT promjenama, uključujući promjene softverskih i hardverskih komponenti, firmvera, sistema i bezbjednosnih parametara, koje su zasnovane na procjeni rizika i predstavljaju sastavni dio opšteg procesa upravljanja promjenama u finansijskom subjektu, kako bi se obezbijedilo da se sve promjene IKT sistema evidentiraju, testiraju, procjenjuju, odobravaju, sprovode i provjeravaju na kontrolisan način; 6) utvrdi i primjenjuje odgovarajuće i sveobuhvatne politike za primjenu softverskih i hardverskih zakrpa i ažuriranja. (5) Finansijski subjekt je dužan da strukturu za upravljanje mrežom i infrastrukturom iz stava 4 tačka 2 ovog člana kreira i implementira na način kojim se omogućava brzo ukidanje ili segmentiranje mrežnog pristupa, kako bi se u najvećoj mogućoj mjeri ograničilo i spriječilo širenje zaraze, a naročito u slučaju međusobno povezanih finansijskih procesa. (6) Struktura za upravljanje mrežom i infrastrukturom iz stava 4 tačka 2 ovog člana može da obuhvati primjenu automatizovanih mehanizama za izolaciju zahvaćene informacione imovine u slučaju sajber napada.	
---	---	--

	(7) Postupak upravljanja IKT promjenama iz stava 4 tačka 5 ovog člana mora biti odobren od strane odgovarajućih linija i nivoa odlučivanja finansijskog subjekta, i mora da se sprovodi u skladu sa posebno utvrđenim protokolima finansijskog subjekta.			
Članak 10. Otkrivanje 1. Finansijski 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.	Praćenje, otkrivanje i analiza IKT događaja i incidenata Član 16, st. 1 i 2 (1) Finansijski subjekt je dužan da uspostavi mehanizme za brzo otkrivanje neuobičajenih aktivnosti, u skladu sa članom 22 ovog zakona, uključujući otkrivanje problema u performansama IKT mreže i IKT incidenata, kao i mehanizme za identifikovanje potencijalnih značajnih jedinstvenih tačaka prekida. (2) Finansijski subjekt je dužan da obezbijedi redovno testiranje mehanizama iz stava 1 ovog člana na način propisan članom 28 ovog zakona.	Potpuno usklađeno		
2. Mehanizmima otkrivanja iz stavka 1. omogućuje se više razina kontrole, utvrđuju pragovi za upozorenja i kriteriji za aktiviranje i pokretanje procesa odgovora na IKT incidente, što uključuje mehanizme za automatsko upozoravanje relevantnog osoblja zaduženog za odgovor na IKT incidente.	Član 16, stav 3 (3) Mehanizmi iz stava 1 ovog člana moraju da omoguće kontrolu na više nivoa, utvrde pragove za dobijanje upozorenja i kriterijume za aktiviranje i započinjanje procesa odgovora na IKT incidente, što uključuje i mehanizme za automatsko obavješćavanje relevantnih lica zaduženih za odgovor na IKT incidente.	Potpuno usklađeno		
3. Finansijski subjekti izdvajaju dostatne resurse i sposobnosti za praćenje aktivnosti korisnika, nastanka neobičnih pojava u IKT-u i IKT incidenata, posebno kibernetičkih.	Član 16, stav 4 (4) Finansijski subjekt je dužan da obezbijedi dovoljne resurse i kapacitete za praćenje aktivnosti korisnika, otkrivanje neuobičajenih IKT događaja i IKT incidenata, a naročito sajber napada.	Potpuno usklađeno		
4. Pružatelji usluga dostave podataka usto uspostavljaju sisteme 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.	Član 16, stav 5 (5) Pružalac usluga dostave podataka dužan je da uspostavi sisteme kojima se može efikasno provjeriti da li su izvješćaji o trgovanju potpuni i kojima se mogu utvrditi propusti i očigledne greške i zahtijevati ponovni prenos tih izvješćaja.	Potpuno usklađeno		
Članak 11. Odgovor i oporavak 1. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. i na temelju zahtjeva u pogledu utvrđivanja iz članka 8., finansijski subjekti uvode sveobuhvatnu politiku kontinuiteta poslovanja u području IKT-a, koja se može donijeti kao zasebna	Kontinuitet poslovanja, odgovor na IKT incidente i oporavak nakon njih Član 17, st. 1 i 2 (1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na osnovu rezultata postupanja u skladu sa članom 14 ovog	Potpuno usklađeno		

namjenska politika koja je sastavni dio opće politike kontinuiteta poslovanja finansijskog subjekta.	zakona, uspostavi sveobuhvatnu IKT politiku kontinuiteta poslovanja. (2) IKT politika kontinuiteta poslovanja iz stava 1 ovog člana predstavlja sastavni dio opšte politike kontinuiteta poslovanja finansijskog subjekta, a može se usvojiti u formi zasebnog, namjenskog akta.			
2. Finansijski 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 finansijskog 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.	Član 17, stav 3 (3) Finansijski subjekt je dužan da IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana primjenjuje pomoću odgovarajućih, namjenskih i dokumentovanih mjera, planova, procedura i mehanizama u cilju: 1) obezbjeđivanja kontinuiteta kritičnih ili važnih funkcija finansijskog subjekta; 2) brzog, adekvatnog i efikasnog odgovora na sve IKT incidente i njihovog rješavanja, na način kojim se ograničava šteta i daje prioritet nastavku poslovanja i oporavku; 3) pokretanja, bez odlaganja, namjenskih planova kojima se, za sve vrste IKT incidenata, omogućava sprovođenje njima prilagođenih mjera, procesa i tehnologija za suzbijanje negativnih efekata i sprečavanje nastanka dalje štete, kao i posebno prilagođenih procedura za odgovor i oporavak iz člana 18 ovog zakona; 4) preliminarne procjene uticaja, štete i gubitaka; 5) utvrđivanja mjera za komunikaciju i upravljanje u kriznim situacijama kojima se obezbjeđuje dostavljanje ažurnih informacija svim relevantnim zaposlenima i eksternim zainteresovanim stranama u skladu sa članom 20 ovog zakona, i za izvješćavanje nadležnog organa u skladu sa odredbama člana 24 ovog zakona.	Potpuno usklađeno		
3. U sklopu okvira za upravljanje IKT rizicima iz članka 6. stavka 1. finansijski subjekti provode povezane planove odgovora i oporavka u području IKT-a, koji, kad je riječ o finansijskim subjektima koji nisu mikropoduzeća, podliježu neovisnim unutarnjim revizijskim pregledima.	Član 17, st. 4 i 5 (4) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje odgovarajuće planove za odgovor i oporavak u IKT oblasti. (5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi nezavisnu internu reviziju planova iz stava 4 ovog člana.	Potpuno usklađeno		

4. Finansijski 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 aranžmana s trećim stranama pružateljima IKT usluga.	Član 17, stav 6 (6) Finansijski subjekt dužan je da uspostavi, održava i periodično testira odgovarajuće IKT planove kontinuiteta poslovanja, naročito za kritične ili važne funkcije koje, na osnovu zaključenih ugovora, obavljaju ili isporučuju treće strane koje pružaju IKT usluge.	Potpuno usklađeno	
5. U sklopu opće politike kontinuiteta poslovanja finansijski subjekti provode analizu učinka na poslovanje (BIA) s obzirom na svoju izloženost ozbiljnim poremećajima u poslovanju. U okviru BIA-e finansijski subjekti procjenjuju mogući učinak ozbiljnih poremećaja u poslovanju s pomoću kvantitativnih i kvalitativnih kriterija, pri čemu se služe unutarnjim i vanjskim podacima 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. Finansijski 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 redundancije svih ključnih komponenta.	Član 17, st. 7 do 11 (7) Finansijski subjekt je dužan da, u okviru opšte politike kontinuiteta poslovanja, sprovodi analizu uticaja na poslovanje odnosno analizu svoje izloženosti ozbiljnim poremećajima u poslovanju. (8) Finansijski subjekt je dužan da, u okviru analize uticaja na poslovanje iz stava 7 ovog člana, na osnovu kvalitativnih i kvantitativnih kriterijuma, korišćenjem raspoloživih internih i eksternih podataka i analize scenarija, procijeni potencijalni uticaj ozbiljnih poremećaja u poslovanju. (9) Finansijski subjekt je dužan da prilikom vršenja analize uticaja na poslovanje iz stava 7 ovog člana uzme u obzir kritičnost identifikovanih poslovnih funkcija, pomoćnih procesa, informacione imovine, zavisnosti od trećih strana, kao i njihovu povezanost i međuzavisnost. (10) Finansijski subjekt je dužan da osmisli i koristi IKT imovinu i IKT usluge na način koji je u potpunosti usklađen sa rezultatima analize uticaja na poslovanje iz stava 7 ovog člana, naročito u pogledu obezbjeđivanja adekvatne redundancije svih kritičnih komponenti. (11) Redundancija, u smislu stava 10 ovog člana, označava postojanje jedne ili više dodatnih komponenti koje preuzimaju funkciju primarne komponente u slučaju njenog prekida rada.	Potpuno usklađeno	
Član 11, stav 6 6. U sklopu sveobuhvatnog upravljanja IKT rizicima finansijski 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;	Član 17, st. 12 do 14 (12) U okviru sveobuhvatnog upravljanja IKT rizicima, finansijski subjekt dužan je da: 1) za IKT sisteme koji podržavaju funkcije finansijskog subjekta, testira planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana i IKT planove kontinuiteta poslovanja iz stava 6 ovog člana: - najmanje jednom godišnje; i	Potpuno usklađeno	

(b) testiraju planove komunikacije u krizi izrađene u skladu s člankom 14. Za potrebe prvog podstavka točke (a) finansijski subjekti koji nisu mikropoduzeća u planove testiranja uključuju scenarije kibernetičkih 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.	- u slučaju značajnih promjena IKT sistema koji podržavaju kritične ili važne funkcije finansijskog subjekta. 2) testira planove komunikacije u kriznim situacijama iz člana 20 ovog zakona. (13) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da testiranjem iz stava 12 tačka 1 ovog člana obuhvati scenarije sajber napada i scenarije prelazaka između primarne IKT infrastrukture i rezervnih kapaciteta, rezervnih kopija podataka, rezervnih sistema i rezervnih lokacija, neophodnih za ispunjavanje zahtjeva iz člana 18 ovog zakona. (14) Finansijski subjekt je dužan da redovno preispituje IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana i planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana, uzimajući u obzir rezultate testiranja iz stava 12 ovog člana, preporuke revizije i zahtjeve nadležnog organa.			
7. Finansijski 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.	Član 17, stav 15 (15) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi odgovorno lice ili organizacionu jedinicu za upravljanje kriznim situacijama koja je, u slučaju pokretanja planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, naročito dužna da utvrdi jasne procedure za upravljanje internom i eksternom komunikacijom u skladu sa članom 20 ovog zakona.	Potpuno usklađeno		
8. U slučaju aktivacije planova kontinuiteta poslovanja u području IKT-a te planova odgovora i oporavka u području IKT-a, finansijski subjekti vode evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna.	Član 17, stav 16 (16) U slučaju pokretanja IKT planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, finansijski subjekt je dužan da vodi evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna.	Potpuno usklađeno		
9. Središnji depozitoriji vrijednosnih papira nadležnim tijelima dostavljaju preslike rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi.	Član 17, stav 18 (18) Centralno klirinško depozitarno društvo dužno je da dostavlja Komisiji kopije rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi.	Potpuno usklađeno		

10. Financijski subjekti koji nisu mikropoduzeća nadležnim tijelima na zahtjev dostavljaju procjenu ukupnih godišnjih troškova i gubitaka prouzročenih značajnim IKT incidentima.	Član 17, stav 17 (17) Financijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi procjenu ukupnih godišnjih troškova i gubitaka koje su prouzrokovali značajni IKT incidenti.	Potpuno usklađeno		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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 sustava i podataka uz minimalno razdoblje prekida rada te ograničene poremećaje u radu i gubitke, finansijski 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.	Politike i procedure za izradu rezervnih kopija podataka i procedure i metode za ponovno uspostavljanje i oporavak Član 18, stav 1 (1) Kako bi se omogućilo ponovno uspostavljanje IKT sistema i povratak podataka uz minimalno trajanje prekida i ograničili poremećaji u radu i gubici, finansijski subjekt dužan je da, u okviru sistema upravljanja IKT rizicima, razvije i usvoji: 1) politike i procedure kojima se, na osnovu kritičnosti informacija i povjerljivosti podataka, utvrđuju obim i minimalna učestalost izrade rezervnih kopija podataka; 2) procedure i metode za povratak, ponovno uspostavljanje i oporavak.	Potpuno usklađeno		
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 sustava 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.	Član 18, st. 2 do 4 (2) Finansijski subjekt je dužan da obezbijedi sisteme za izradu rezervnih kopija podataka koji se mogu koristiti u skladu sa politikama i procedurama za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i u skladu sa procedurama i metodama za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana. (3) Korišćenjem sistema za izradu rezervnih kopija podataka iz stava 2 ovog člana ne smije se ugroziti bezbjednost mrežnih i informacijskih sistema ni dostupnost, autentičnost, integritet ili povjerljivost podataka. (4) Finansijski subjekt je dužan da periodično testira procedure za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i	Potpuno usklađeno		

	procedure i metode za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana.			
3. Pri vraćanju podataka sa sigurnosne kopije s pomoću vlastitih sustava finansijski 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.	Član 18, st. 5 i 6 (5) Kada finansijski subjekt koristi sopstvene sisteme za povraćaj podataka iz rezervnih kopija, dužan je da obezbijedi da se za te potrebe koriste IKT sistemi koji su fizički i logički odvojeni od izvornih IKT sistema iz kojih podaci potiču. (6) IKT sistemi iz stava 5 ovog člana koji su namijenjeni za oporavak, moraju biti bezbjedno zaštićeni od neovlaštenog pristupa i IKT kompromitacija i omogućiti blagovremeno ponovno uspostavljanje usluga, pri čemu se, po potrebi, koriste rezervne kopije podataka i sistema. Član 18, st. 13 i 14 (13) Centralna druga ugovorena strana dužna je da uspostavi planove koji moraju omogućiti oporavak svih transakcija koje su bile u toku u trenutku nastanka poremećaja, kako bi se obezbijedio nesmetan i siguran nastavak poslovanja centralne druge ugovorne strane i omogućilo izvršenje obaveza na predviđeni datum. (14) Pružalac usluga dostave podataka dužan je da obezbijedi odgovarajuće resurse i infrastrukturu za izradu rezervnih kopija i obnovu sistema, radi kontinuiranog pružanja i održavanja svojih usluga.	Potpuno usklađeno		
4. Finansijski 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.	Član 18, st. 7 i 8 (7) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da održava rezervne IKT kapacitete koji imaju resurse, sposobnosti i funkcije dovoljne za adekvatno obezbjeđivanje potreba poslovnih procesa. (8) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da, u skladu sa svojim rizičnim profilom, procijeni potrebu održavanja rezervnih IKT kapaciteta iz stava 7 ovog člana.	Potpuno usklađeno		
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:	Član 18, st. 15 i 16 (15) Centralno klirinško depozitarno društvo dužno je održavati najmanje jedno sekundarno mjesto obrade, opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem, kako bi se zadovoljile poslovne potrebe.	Potpuno usklađeno		

(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 pružiti 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.	(16) Sekundarno mjesto obrade iz stava 15 ovog člana: 1) mora biti geografski udaljeno od primarnog mjesta obrade kako bi se osigurao različit profil rizika i spriječilo da bude pogođeno istim događajem koji je zahvatio primarno mjesto; 2) mora omogućavati kontinuitet kritičnih ili važnih funkcija na način identičan primarnom mjestu ili pružati nivo usluga potreban za izvršenje ključnih operacija financijskog subjekta u skladu sa ciljevima oporavka; 3) mora biti odmah dostupno osoblju financijskog subjekta kako bi se osigurao kontinuitet kritičnih 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.	Član 18, st. 9 i 10 (9) Financijski subjekt je dužan da, prilikom određivanja ciljnih vremena oporavka i ciljnih tačaka oporavka za svaku funkciju, uzme u obzir značaj te funkcije, a naročito da li se radi o kritičnoj ili važnoj funkciji, kao i potencijalni ukupni uticaj ciljeva oporavka na efikasnost tržišta. (10) Ciljno vrijeme oporavka i ciljna tačka oporavka iz stava 9 ovog člana moraju biti takvi da, u ekstremnim scenarijima, obezbjeđuju ispunjavanje dogovorenih nivoa usluga.	Potpuno usklađeno		
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.	Član 18, st. 11 i 12 (11) Prilikom oporavka od IKT incidenta, financijski subjekt je dužan da sprovede sve neophodne kontrole, uključujući višestruke provjere i usklađivanja, kako bi obezbijedio održavanje najvišeg nivoa integriteta podataka. (12) Kontrole iz stava 11 ovog člana moraju se sprovoditi i prilikom rekonstrukcije podataka iz eksternih izvora, radi obezbjeđivanja usklađenosti svih podataka između sistema.	Potpuno usklađeno		
Članak 13. Učenje i razvoj 1. Financijski subjekti raspolažu sposobnostima i osobljem za prikupljanje informacija o ranjivostima i kiberprijetnjama, IKT incidentima, a osobito kibernetičkim napadima, te za analizu njihova vjerovatnog učinka na digitalnu operativnu otpornost financijskih subjekata.	Usavršavanje u cilju jačanja digitalne operativne otpornosti Član 19, stav 1 (1) Financijski subjekt je dužan da obezbijedi kapacitete i odredi lica zadužena za prikupljanje informacija o ranjivostima, sajber prijetnjama, IKT incidentima, a naročito o sajber napadima, kao i za analizu njihovog mogućeg uticaja na digitalnu operativnu otpornost financijskog subjekta.	Potpuno usklađeno		

2. Finansijski subjekti uvođe 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. Finansijski 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 podstavka 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 finansijskog subjekta; (d) djelotvornosti unutarnje i vanjske komunikacije.	Član 19, st. 2 do 4 (2) Finansijski subjekt je dužan da uspostavi proces naknadne analize IKT incidenata, koji se sprovodi nakon što značajan IKT incident poremeti obavljanje njegovih osnovnih aktivnosti, u cilju analize uzroka poremećaja i utvrđivanja potrebnih poboljšanja u IKT operacijama ili u IKT politici kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona. (3) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi informacije o izmjenama koje su sprovedene nakon analize IKT incidenta iz stava 2 ovog člana. (4) Naknadnom analizom IKT incidenta iz stava 2 ovog člana mora se utvrditi da li su uspostavljene procedure bile ispoštovane i da li su preduzete mjere bile djelotvorne, uključujući: 1) brzinu reagovanja na bezbjednosna upozorenja i utvrđivanja uticaja IKT incidenta i njegove ozbiljnosti; 2) kvalitet i brzinu sprovođenja forenzičke analize, u slučajevima kada je to svrsishodno; 3) efikasnost interne eskalacije incidenta; 4) efikasnost interne i eksterne komunikacije.	Potpuno usklađeno		
3. Pouke stečene iz testiranja digitalne operativne otpornosti provedenog u skladu s člancima 26. i 27. te iz stvarnih IKT incidenata, osobito kibernetičkih, 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 finansijskim subjektima i procijenjenima tijekom nadzornih preispitivanja, propisno se i kontinuirano uključuju u proces procjene IKT rizika. Na temelju tih nalaza provode se odgovarajuća preispitivanja relevantnih komponenata okvira za upravljanje IKT rizicima iz članka 6. stavka 1.	Član 19, st. 5 i 6 (5) Finansijski subjekt je dužan da obezbijedi da se iskustva stečena kroz testiranje digitalne operativne otpornosti iz čl. 27 do 32 ovog zakona, kao i iz nastalih IKT incidenata, a naročito sajber napada, saznanja o izazovima koji su se pojavili prilikom pokretanja planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona, relevantne informacije dobijene od drugih subjekata, kao i informacije u vezi sa zahtjevima nadležnog organa, blagovremeno, adekvatno i kontinuirano koriste u okviru procesa procjene IKT rizika. (6) Finansijski subjekt je dužan da iskustva, saznanja i informacije iz stava 5 ovog člana, na odgovarajući način, uzme u obzir prilikom preispitivanja relevantnih komponenti sistema upravljanja IKT rizicima.	Potpuno usklađeno		

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, razmjere i razvoj IKT incidenata, osobito kibernetičkih, 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.	Član 19, st. 7 i 8 (7) Financijski subjekt je dužan da prati efikasnost sprovođenja strategije digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona. (8) Financijski subjekt je dužan da evidentira i prati promjenu ukupnog profila IKT rizika tokom vremena, analizira učestalost, vrste, razmjere i trendove IKT incidenata, a naročito sajber napada i njihovih obrazaca, kako bi razumio nivo svoje izloženosti IKT riziku, posebno u odnosu na kritične ili važne funkcije i unaprijedio stepen svoje zrelosti i spremnosti u oblasti sajber bezbjednosti.	Potpuno usklađeno		
5. Više IKT osoblje najmanje jedanput godišnje izvješćuje upravljačko tijelo o nalazima iz stavka 3. te iznosi preporuke.	Član 19, stav 9 (9) Financijski subjekt je dužan da obezbijedi da viši IKT kadar, najmanje jednom godišnje, podnosi izvještaj organu upravljanja o zaključcima izvedenim iz iskustava, saznanja i informacija iz stava 5 ovog člana, sa predlozima za dalje postupanje.	Potpuno usklađeno		
6. Financijski subjekti osmišljavaju programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti kao obavezne 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. tačkom i.	Član 19, st. 10 do 12 (10) Financijski subjekt je dužan da osmisli i sprovodi programe za podizanje svijesti o IKT bezbjednosti i obuke o digitalnoj operativnoj otpornosti, kao obavezne djelove svojih programa obuke zaposlenih. (11) Programi i obuke iz stava 10 ovog člana primjenjuju se na sve zaposlene i članove višeg rukovodstva, a nivo njihove složenosti mora biti prilagođen nadležnostima i poslovima koje ta lica obavljaju. (12) Financijski subjekt je dužan da, kada je to primjenljivo, uključi treće strane koje pružaju IKT usluge u odgovarajuće programe obuke, u skladu sa članom 38 stav 3 tačka 11 ovog zakona.	Potpuno usklađeno		
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 kibernetičkih napada.	Član 19, st. 13 i 14 (13) Financijski subjekt, koji nije klasifikovan kao mikro financijski subjekt, dužan je da kontinuirano prati trendove u razvoju tehnologija, kako bi bolje razumio mogući uticaj primjene novih tehnologija na zahtjeve u oblasti IKT bezbjednosti i digitalnu operativnu otpornost. (14) Financijski subjekt, koji nije klasifikovan kao mikro financijski subjekt, dužan je da bude upoznat sa najnovijim metodama za upravljanje IKT rizicima, kako bi mogao efikasno da odgovori na postojeće i nove oblike sajber napada.	Potpuno usklađeno		

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.	Komunikacija u kriznim situacijama Član 20, stav 1 (1) Financijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi planove komunikacije u kriznim situacijama, koji omogućavaju da na odgovoran način saopštava informacije, najmanje o značajnim IKT incidentima i značajnim ranjivostima, klijentima, poslovnim partnerima i široj javnosti, u zavisnosti od slučaja.	Potpuno usklađeno		
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.	Član 20, st. 2 i 3 (2) Financijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje politike komunikacije za zaposlene i sa eksternim zainteresovanim stranama. (3) Politike komunikacije iz stava 2 ovog člana, u dijelu koji se odnosi na zaposlene, moraju uzeti u obzir da se mora praviti razlika između zaposlenih koje je potrebno samo informisati i zaposlenih koji učestvuju u upravljanju IKT rizicima, odnosno koji su zaduženi za odgovor i oporavak.	Potpuno usklađeno		
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.	Član 20, stav 4 (4) Najmanje jedno lice u financijskom subjektu mora biti zaduženo za sprovođenje strategije komunikacije u slučaju IKT incidenata i da, u tu svrhu, obavlja poslove informisanja medija i javnosti.	Potpuno usklađeno		
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 osigurala 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;	Nema odgovarajuće odredbe	Neprenosivo		

(b) dodatno razradile komponente kontrole prava 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 opisale 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 nacrt 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 usmjerene 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;	Pojednostavljeni sistem upravljanja IKT rizicima Član 21 (1) Odredbe čl. 8 do 19 ovog zakona ne primjenjuju se na malo i nepovezano investiciono društvo i malu instituciju za profesionalnu penzionu štednju. (2) Finansijski subjekti iz stava 1 ovoga člana dužni su da: 1) uspostave i održavaju pouzdan i dokumentovan sistem upravljanja IKT rizikom, koji detaljno opisuje mehanizme i mjere usmjerene na brzo, efikasno i sveobuhvatno upravljanje IKT rizikom, uključujući i zaštitu relevantnih fizičkih komponenti i infrastrukture; 2) kontinuirano prate bezbjednost i funkcionisanje svih IKT sistema; 3) minimiziraju uticaj IKT rizika korišćenjem pouzdanih, otpornih i ažurnih IKT sistema, protokola i alata koji su primjereni za podršku obavljanju njihovih aktivnosti i pružanju usluga, kao i za adekvatnu zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka u mrežnim i informacionim sistemima; 4) omoguće pravovremeno identifikovanje izvora IKT rizika i anomalija u mrežnim i informacionim sistemima, kao i brzo postupanje u slučaju IKT incidenata; 5) identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge; 6) obezbijede kontinuitet kritičnih ili važnih funkcija pomoću planova kontinuiteta poslovanja i mjera odgovora i oporavka, koje uključuju najmanje mjere izrade rezervnih kopija podataka i povraćaja podataka iz rezervnih kopija; 7) redovno testiraju efikasnost kontrola koje se sprovode u skladu sa tač. 1 i 3, kao i planove i mjere iz tačke 6 ovog stava; 8) u skladu sa potrebama i profilom IKT rizika, koriste relevantne operativne zaključke koji proizlaze iz testiranja iz tačke 7 ovog	Potpuno usklađeno	Usklađivanje je izvršeno za sve subjekte iz stava 1 koji postoje u Crnoj Gori.	Odrađen je reg. maksimum, dalje usklađivanje je moguće samo po pristupanju.
			Opcija/diskrecija da se Razvojna banka Crne Gore izuzme od primjene zakona je iskorištena, pa se ona zbog toga ne navodi u stavu 1	

(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.	stava i analiza nakon incidenata u procesu procjene IKT rizika, kao i da razvijaju programe za podizanje svijesti o IKT bezbjednosti i obuke iz oblasti digitalne operativne otpornosti za zaposlene 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.	Propisi Komisije o digitalnoj operativnoj otpornosti Član 49 stav 9 (9) Komisija bliže propisuje kriterijume za pojednostavljeni sistem upravljanja IKT rizicima iz člana 21 ovog zakona.	Djelimično usklađeno	Potpuno usklađivanje će se izvršiti kroz podzakonski akt Komisije za tržište kapitala Crne Gore iz člana 49 stav 9	II kvartal 2027
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);	Nema odgovarajuće odredbe	Neprenosivo		

(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 nacrt 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.	III. UPRAVLJANJE, KLASIFIKACIJA I IZVJEŠTAVANJE O IKT INCIDENTIMA Proces upravljanja IKT incidentima Član 22, stav 1 (1) Financijski subjekt je dužan da definiše, uspostavi i primijeni proces upravljanja IKT incidentima radi otkrivanja, upravljanja i obavješćivanja o IKT incidentima.	Potpuno usklađeno		
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.	Član 22, st. 2 i 3 (2) Financijski subjekt je dužan da evidentira sve IKT incidente i ozbiljne sajber prijetnje. (3) Financijski subjekt je dužan da uspostavi adekvatne procedure i postupke kojima se obezbjeđuje da se, na dosljedan i objedinjen način postupa sa IKT incidentima, vrši njihovo praćenje i preduzimaju dalje mjere, kako bi se obezbijedilo da se osnovni uzroci IKT incidenata identifikuju, dokumentuju i tretiraju, radi sprečavanja ponavljanja takvih incidenata.	Potpuno usklađeno		

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.	Član 22, stav 4 (4) Financijski subjekt je dužan da, u okviru procesa upravljanja IKT incidentima iz stava 1 ovog člana: 1) uspostavi indikatore ranog upozorenja; 2) uspostavi procedure za identifikaciju, praćenje, evidentiranje, kategorizaciju i klasifikaciju IKT incidenata prema njihovom prioritetu i nivou ozbiljnosti, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona, uzimajući u obzir kritičnost usluga zahvaćenih incidentom; 3) dodijeli zaduženja i odgovornosti za postupanje u slučaju različitih IKT incidenata, prema njihovim vrstama i scenarijima; 4) utvrdi planove za komunikaciju sa zaposlenima, eksternim zainteresovanim stranama i medijima u skladu sa članom 20 ovog zakona, planove za obavješćivanje klijenata, za postupke interne eskalacije incidenata, uključujući prigovore klijenata povezane sa IKT-om, kao i za informisanje drugih finansijskih subjekata sa kojima ima poslovnu saradnju, kada je to primjenljivo; 5) obezbijedi da se više rukovodstvo i organ upravljanja izvještavaju najmanje o značajnim IKT incidentima, uz obrazloženje njihovog uticaja, odgovora na njih i dodatnih kontrola koje je potrebno uspostaviti zbog nastanka takvih IKT incidenata; 6) uspostavi procedure za odgovor na IKT incidente, kako bi ublažio njihov uticaj i obezbijedio da usluge zahvaćene incidentom ponovo, blagovremeno postanu dostupne, funkcionalne i bezbjedne.	Potpuno usklađeno	
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 primjenljivo, količine ili broja transakcija zahvaćenih IKT incidentom te činjenice je li IKT incident imao učinak na ugled financijskog subjekta;	Klasifikacija IKT incidenata i sajber prijetnji Član 23, stav 1 (1) Financijski subjekt je dužan da klasifikuje IKT incidente i da utvrdi njihov uticaj na osnovu sljedećih kriterijuma: 1) broja i/ili značaja klijenata zahvaćenih IKT incidentom, ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana zahvaćena incidentom i, kada je to primjenljivo, vrijednosti ili broja transakcija zahvaćenih incidentom, kao i činjenice da li je incident narušio ugled finansijskog subjekta;	Potpuno usklađeno	

(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) trajanja IKT incidenta, uključujući period prekida pružanja usluge; 3) geografske rasprostranjenosti u smislu područja koje je IKT incident zahvatio, naročito ako je zahvatio više od dvije države članice; 4) gubitka svojstva podataka uslijed IKT incidenta, odnosno gubitka dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka; 5) kritičnosti usluga zahvaćenih incidentom, uključujući u pogledu transakcija i operacija financijskog subjekta; 6) ekonomskog uticaja IKT incidenta, odnosno direktnih i indirektnih troškova i gubitaka, u apsolutnom i 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	Klasifikacija IKT incidenata i sajber prijetnji Član 23, stav 2 (2) Financijski subjekt je dužan da klasifikuje sajber prijetnje kao ozbiljne na osnovu kritičnosti usluga koje su izložene riziku, uključujući u pogledu transakcija i operacija financijskog subjekta, broja i/ili značaja klijenata izloženih tom riziku ili broja i/ili značaja financijskih subjekata i institucija koje su druga ugovorna strana izložena tom riziku i geografske rasprostranjenosti u smislu područja izloženih riziku.	Potpuno usklađeno		
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	Nema odgovarajuće odredbe	Neprenosivo		

IKT incidentima ili, ovisno o slučaju, značajnim operativnim ili sigurnosnim incidentima povezanim 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 nacrt 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.	Nema odgovarajuće odredbe	Neprenosivo		
Članak 19. Izvrješćivanje o značajnim IKT incidentima i dobrovoljno obavješćivanje o ozbiljnim kiberprijetnjama 1. Financijski subjekti izvrješćuju 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 izvrješćuju relevantno nacionalno	Izvrješćivanje o značajnim IKT incidentima i obavješćivanje o ozbiljnim sajber prijetnjama Član 24, st. 1 do 5 (1) Finansijski subjekt je dužan da o značajnom IKT incidentu izvrješćava nadležni organ. (2) Radi izvrješćavanja iz stava 1 ovog člana, finansijski subjekt je dužan da prikupi i analizira sve relevantne informacije o značajnom IKT incidentu, pripremi dokumentaciju iz stava 3 ovog člana i dostavi je nadležnom organu na način i u roku utvrđenom posebnim propisom nadležnog organa. (3) Finansijski subjekt je dužan da nadležnom organu dostavi: 1) početno obavješćenje;	Djelimično usklađeno	Odredba koja se odnosi na kreditne institucije koje su u skladu sa članom 6 stav 4 Regulative (EU) br. 1024/2013 klasifikovane kao značajne je neprenosiva jer Crna Gora	Po pristupan ju Crne Gore EU i nakon što SSM bude prepozna t u posebno m propisu

nadležno tijelo imenovano u skladu s člankom 4. Direktive 2013/36/EU, koje to izvješće odmah proslijeđuje ESB-u. Za potrebe prvog podstavka finansijski 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, finansijski 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 finansijskog subjekta na temelju prvog podstavka, države članice povrh toga mogu odrediti da neki ili svi finansijski 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) imenovanim ili uspostavljenim u skladu s Direktivom (EU) 2022/2555.	2) prelazni izvještaj nakon početnog obavještenja iz tačke 1 ovog stava, čim dođe do značajne promjene u statusu prijavljenog značajnog IKT incidenta ili promjene u postupanju sa tim incidentom u skladu sa novim dostupnim informacijama, a nakon toga, po potrebi, ažurirane prelazne izvještaje u slučaju bitne promjene statusa incidenta, kao i na izričit zahtjev nadležnog organa; 3) završni izvještaj, nakon što izvrši analizu osnovnog uzroka incidenta, bez obzira na to da li su mjere za ublažavanje njegovog uticaja već sprovedene, i kada su dostupni konačni podaci o uticaju incidenta, a kojima se mogu zamijeniti prethodne procjene. (4) Dokumentacija iz stava 3 ovog člana mora sadržati sve informacije koje su nadležnom organu potrebne da utvrdi ozbiljnost značajnog IKT incidenta i procijeni mogućnost prekograničnog uticaja tog incidenta. (5) Izuzetno od stava 2 ovog člana, u slučaju da finansijski subjekt zbog tehničkih poteškoća nije u mogućnosti da dostavi početno obavještenje iz stava 3 ovog člana na način utvrđen posebnim propisom nadležnog organa, dostavljanje se može izvršiti na drugi pogodan način.		nije dio SSM-a (Eng. Single Supervisory Mechanism) Opcija/diskrecija za paralelno izvješćivanje organa utvrđenih u Zakonu o informacionoj bezbjednosti nije iskorištena	
2. Finansijski subjekti mogu, na dobrovoljnoj osnovi, obavijestiti relevantno nadležno tijelo o ozbiljnim kiberprijetnjama ako smatraju da je prijetnja relevantna za finansijski 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 proslijeđuje ESB-u. Države članice mogu odrediti da oni finansijski subjekti koji dostave obavijest na dobrovoljnoj osnovi u skladu s prvim podstavkom tu obavijest također mogu proslijediti CSIRT-ovima	Član 24, st. 6 i 7 (6) Finansijski subjekt može da obavijesti nadležni organ o ozbiljnoj sajber prijetnji kada procijeni da je prijetnja relevantna za finansijski sistem, korisnike usluga ili klijente. (7) Nadležni organ može da dostavi informacije o ozbiljnoj sajber prijetnji iz stava 6 ovog člana organima iz stava 11 ovog člana.	Djelimično usklađeno	Odredba koja se odnosi na kreditne institucije koje su u skladu sa članom 6 stav 4 Regulative (EU) br. 1024/2013 klasifikovane kao značajne je neprenosiva jer Crna Gora nije dio SSM-a	Po pristupanju Crne Gore EU i nakon što SSM bude prepoznat u posebno m propisu

imenovanima ili uspostavljenima u skladu s Direktivom (EU) 2022/2555.			(Eng. Single Supervisory Mechanism)	
			Opcija/diskrecija za paralelno izvještavanje organa utvrđenih u Zakonu o informacionoj bezbjednosti nije iskorištena	
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 primjenljivo, obavješćuju svoje klijente koji bi njome mogli biti zahvaćeni o svim odgovarajućim zaštitnim mjerama čije bi poduzimanje klijenti mogli razmotriti.	Član 24, st. 8 i 9 (8) Kada nastane značajan IKT incident koji utiče na financijske interese klijenata, finansijski subjekt dužan je da, bez odlaganja, odmah po saznanju za takav incident, obavijesti klijente o tom incidentu i o mjerama preduzetim za ublažavanje negativnih uticaja tog incidenta. (9) U slučaju ozbiljne sajber prijetnje, finansijski subjekt je dužan da, kada je to primjenljivo, obavijesti klijente na koje bi ta prijetnja mogla da utiče o mjerama zaštite koje mogu da preduzmu.	Potpuno usklađeno		
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;	Član 24, stav 2 i 3 (2) Radi izvještavanja iz stava 1 ovog člana, finansijski subjekt je dužan da prikupi i analizira sve relevantne informacije o značajnom IKT incidentu, pripremi dokumentaciju iz stava 3 ovog člana i dostavi je nadležnom organu na način i u roku utvrđenom posebnim propisom nadležnog organa. (3) Finansijski subjekt je dužan da nadležnom organu dostavi: 1) početno obavještenje; 2) prelazni izvještaj nakon početnog obavještenja iz tačke 1 ovog stava, čim dođe do značajne promjene u statusu prijavljenog značajnog IKT incidenta ili promjene u postupanju sa tim	Potpuno usklađeno		

(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.	incidentom u skladu sa novim dostupnim informacijama, a nakon toga, po potrebi, ažurirane prelazne izvještaje u slučaju bitne promjene statusa incidenta, kao i na izričit zahtjev nadležnog organa; 3) završni izvještaj, nakon što izvrši analizu osnovnog uzroka incidenta, bez obzira na to da li su mjere za ublažavanje njegovog uticaja već sprovedene, i kada su dostupni konačni podaci o uticaju incidenta, a kojima se mogu zamijeniti prethodne procjene.			
5. Finansijski 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 finansijski subjekt ostaje u potpunosti odgovoran za ispunjavanje zahtjeva u pogledu izvješćivanja o incidentima.	Član 24, stav 10 (10) Finansijski subjekt može, u skladu sa zakonom, da povjeri trećoj strani obavljanje poslova obavješćivanja u skladu sa ovim članom, pri čemu je taj finansijski subjekt odgovoran za usklađenost sa odredbama ovog člana.	Potpuno usklađeno		
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 finansijskim subjektima iz članka 2. stavka 1. točaka (a), (b) i (d); (c) nadležnim tijelima, jedinstvenim kontaktnim točkama ili CSIRT-ovima imenovanim 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.	Član 24, stav 11 (11) Po prijemu početnog obavješćenja i svakog izvješća iz stava 3 ovog člana, nadležni organ blagovremeno dostavlja podatke o značajnom IKT incidentu, kada je to primjenljivo, a u skladu sa njihovim nadležnostima: 1) EBA-i, ESMA-i ili EIOPA-i; 2) ECB-u, u slučaju finansijskih subjekata iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona; 3) organu koji je, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, nadležan za zaštitu finansijskog subjekta od sajber prijetnji i incidenata; 4) organu koji je, u skladu sa zakonom kojim se uređuje sanacija kreditnih institucija, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje kritičnih funkcija u smislu tog zakona; 5) organu koji je, u skladu sa zakonom kojim se uređuje sanacija investicionih društava, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje ključnih funkcija u smislu tog zakona; 6) drugom javnom organu, u skladu sa zakonom.	Djelimično usklađeno	Odredba koja se odnosi na obavješćivanje SRB-a (Eng. Single Resolution Board) je neprenosiva jer Crna Gora nije dio SRM-a (Eng. Single resolution mechanism)	Po pristupanju Crne Gore EU i nakon što SSM bude prepoznat u posebnom propisu

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.	Član 24, stav 12 (12) Nadležni organ je dužan da surađuje sa EBA-om, ESMA-om, EIOPA-om i/ili ECB-om u postupku iz člana 19 stav 7 Regulative (EU) br. 2022/2554, koji ti organi sprovode radi procjene relevantnosti značajnog IKT incidenta za nadležne organe u drugim državama članicama, u skladu sa kriterijumima iz člana 11 Regulative (EU) br. 2024/1772. (13) U slučaju da, u skladu sa članom 19 stav 7 Regulative (EU) br. 2022/2554, putem ESCB-a primi obavještenje od ECB-a o pitanjima koja su od značaja za platni sistem, Centralna banka za finansijski subjekt iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona, kada je to primjenljivo, preduzima sve neophodne mjere za zaštitu stabilnosti finansijskog sistema.	Potpuno usklađeno	Odredbe koje se direktno odnose na obaveze EBA-e, ESMA-e, EIOPA-e, ECB-a i ENISA-e su neprenosive	
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.	Član 24, stav 14 (14) Komisija obavještava relevantni nadležni organ države članice domaćina o značajnom IKT incidentu u slučaju kada Centralno klirinško depozitarno društvo ima značajnu prekograničnu aktivnost u toj državi članici domaćina, kada je vjerovatno da će značajni IKT incident imati ozbiljne posljedice po finansijska tržišta države članice domaćina, kao i u situacijama u kojima postoje aranžmani o saradnji među nadležnim organima u vezi sa nadzorom finansijskih subjekata.	Potpuno usklađeno	Odredbe koje se direktno odnose na obaveze ESMA-e su neprenosive	
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.	Nema odgovarajuće odredbe	Neprenosivo		

Pri izradi tog nacrtu 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 odstupa 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	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
3. Europska nadzorna tijela izvješće iz stavka 1. dostavljaju Europskom parlamentu, Vijeću i Komisiji do 17. siječnja 2025.	Nema odgovarajuće odredbe	Neprenosivo		
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	Povratne informacije nadležnog organa Član 25, st. 1 do 4 (1) Nadležni organ je dužan da po prijemu dokumentacije iz člana 24 stav 3 ovog zakona, financijskom subjektu potvrdi prijem. (2) Po prijemu početnog obavještenja i svakog izvješća iz člana 24 stav 3 ovog zakona, nadležni organ može, kada je to moguće, financijskom subjektu blagovremeno pružiti relevantne i srazmjerne informacije ili opšte smjernice za dalje postupanje, naročito davanjem na uvid svih relevantnih anonimizovanih informacija i saznanja o sličnim prijetnjama, kao i da sa tim financijskim subjektom razmotri primijenjene korektivne mjere, načine za ublažavanje i umanjenje negativnih uticaja značajnog IKT incidenta na finansijski sektor u cjelini. (3) Aktivnostima nadležnog organa iz stava 2 ovog člana ne dovode se u pitanje tehnički doprinosi, smjernice, korektivne mjere i dalja	Potpuno usklađeno		

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 izvješćeno u skladu s člankom 19. stavkom 1. i za posljedice tih IKT incidenata.	postupanja koja, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, pružaju i sprovode organi određeni tim zakonom. (4) U slučaju iz stava 2 ovog člana, finansijski subjekt je u potpunosti odgovoran za postupanje sa značajnim IKT incidentom i za njegove posljedice.			
2. Europska nadzorna tijela u okviru Zajedničkog odbora svake godine sastavljaju anonimizirano i agregirano izvješće o značajnim IKT incidentima, pri čemu pojednosti 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.	Nema odgovarajuće odredbe	Neprenosivo		
Članak 23. Operativni ili sigurnosni incidenti povezani sa 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.	Operativni i sigurnosni incidenti povezani sa plaćanjem Član 26 Finansijski subjekti iz člana 2 stav 1 tač. 1 do 4 ovog zakona, dužni su da u slučaju operativnih i sigurnosnih incidenata povezanih sa plaćanjem, uključujući i značajne operativne i sigurnosne incidente povezane sa plaćanjem, shodno primjenjuju odredbe čl. 22 do 25 ovog zakona.	Potpuno usklađeno		
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	IV. TESTIRANJE DIGITALNE OPERATIVNE OTPORNOSTI Opšti zahtjevi za sprovođenje testiranja digitalne operativne otpornosti Član 27, stav 1 (1) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, a u cilju procjene spremnosti za upravljanje IKT incidentima, identifikovanja slabosti, nedostataka i odstupanja u	Potpuno usklađeno		

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.	digitalnoj operativnoj otpornosti i blagovremenog sprovođenja korektivnih mjera, da uspostavi, održava i redovno preispituje program za testiranje digitalne operativne otpornosti.			
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.	Član 27, stav 2 (2) Program za testiranje digitalne operativne otpornosti iz stava 1 ovog člana, kao dio okvira za upravljanje IKT rizicima, mora biti efikasan i sveobuhvatan i sadržati niz procjena, testova, metodologija, praksi i alata koji se sprovode i primjenjuju u skladu sa čl. 28 do 31 ovog zakona.	Potpuno usklađeno		
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.	Član 27, stav 3 (3) Finansijski subjekt iz stava 1 ovog člana, dužan je da sprovodi program za testiranje digitalne operativne otpornosti primjenom pristupa zasnovanog na procjeni rizika, pri čemu mora voditi računa o promjenljivom karakteru IKT rizika, konkretnim rizicima kojima je izložen ili bi mogao biti izložen, kritičnosti informacione imovine i usluga, kao i o svim drugim relevantnim faktorima.	Potpuno usklađeno		
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.	Član 27, st. 4 i 5 4) Finansijski subjekt je dužan da obezbijedi da testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode nezavisna interna ili eksterna lica. (5) U slučaju kada testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode interna lica, finansijski subjekt je dužan da za te potrebe obezbijedi dovoljne resurse i preduzme mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja tog testiranja.	Potpuno usklađeno		
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, nedostaci ili odstupanja u potpunosti otklone.	Član 27, stav 6 (6) Finansijski subjekt iz stava 1 ovog člana, dužan je da uspostavi politike i procedure za određivanje prioriteta, klasifikacije i otklanjanje svih problema otkrivenih tokom testiranja digitalne operativne otpornosti, kao i metodologije za internu provjeru radi	Potpuno usklađeno		

	dobijanja potvrde da su sve identifikovane slabosti, nedostaci i odstupanja u potpunosti otklonjeni.			
6. Finansijski 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.	Član 27, stav 7 (7) Finansijski subjekt iz stava 1 ovog člana, dužan je da najmanje jednom godišnje, sprovodi adekvatne testove svih IKT sistema i aplikacija koje podržavaju kritične ili važne funkcije tog finansijskog subjekta.	Potpuno usklađeno		
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.	Testiranje IKT alata i sistema Član 28, stav 1 (1) Programom za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona mora se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, obezbijediti sprovođenje odgovarajućih testova, kao što su: 1) procjene i skeniranja ranjivosti; 2) analize javno dostupnih izvora; 3) procjene bezbjednosti mreže; 4) analize odstupanja; 5) preispitivanja fizičke bezbjednosti; 6) upitnici i softverska rješenja za skeniranje; 7) pregledi izvornog koda, kada je to izvodljivo; 8) testiranja zasnovana na scenarijima; 9) testiranja kompatibilnosti; 10) testiranja performansi; 11) testiranja od kraja do kraja (eng. end-to-end), odnosno kroz sve faze rada; 12) penetraciona testiranja.	Potpuno usklađeno		
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 komponenta te IKT usluga kojima se podupiru ključne ili važne funkcije finansijskog subjekta.	Član 28, stav 3 (3) Centralno klirinško depozitarno društvo i Centralna druga ugovorna strana, dužni su da sprovode procjene ranjivosti prije svake primjene ili ponovne primjene novih ili postojećih aplikacija, infrastrukturnih komponenti i IKT usluga koje podržavaju kritične ili važne funkcije finansijskog subjekta.	Potpuno usklađeno		
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	Član 28, stav 2 (2) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt, dužan je da testiranja iz stava 1 ovog člana sprovodi	Potpuno usklađeno		

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.	primjenom pristupa zasnovanog na procjeni rizika u skladu sa strateškim planiranjem testiranja u IKT oblasti, uzimajući u obzir potrebu za održavanje uravnoteženog pristupa između obima resursa i vremena potrebnog za sprovođenje testiranja u IKT oblasti, sa jedne strane, i hitnosti, vrste rizika, kritičnosti informacione imovine i usluga, kao i drugih relevantnih faktora, uključujući sposobnost tog financijskog subjekta da preuzme proračunate rizike, sa druge strane.			
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.	Napredno testiranje IKT alata, sustava i procesa zasnovano na TLPT-u Član 29, st. 1, 2 i 4 (1) Financijski subjekt iz stava 4 ovog člana, dužan je da sprovodi napredno testiranje u formi penetracionog testiranja vođenog prijetnjama (u daljem tekstu: TLPT), najmanje jednom u tri godine. (2) Izuzetno od stava 1 ovog člana, nadležni organ može, uzimajući u obzir rizični profil financijskog subjekta i operativne okolnosti, da financijskom subjektu utvrdi obavezu promijene učestalosti naprednog testiranja. (4) Nadležni organ određuje financijske subjekte, koji nisu klasifikovani kao mikro financijski subjekti i nisu subjekti iz člana 21 stav 1 ovog zakona, koji su dužni da sprovode TLPT iz stava 1 ovog člana, uzimajući u obzir princip proporcionalnosti iz člana 5 ovog zakona, na osnovu procjene: 1) uticaja aktivnosti i usluga financijskog subjekta na financijski sektor; 2) mogućih rizika po finansijsku stabilnost, uzimajući u obzir sistemski značaj finansijskog subjekta na: - nacionalnom nivou; - nivou Evropske unije, kada je to primjenljivo. 3) profila IKT rizika finansijskog subjekta, nivoa njegove zrelosti u IKT oblasti i karakteristika tehnologije koju koristi.	Potpuno usklađeno		
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.	Član 29, st. 3, 6 i 7 (3) TLPT iz stava 1 ovog člana mora obuhvatiti više kritičnih ili važnih funkcija finansijskog subjekta ili sve takve funkcije, i sprovodi se na produkcijskim sistemima koji podržavaju te funkcije.	Potpuno usklađeno		

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.	(6) Za potrebe planiranja i sprovođenja TLPT-a iz stava 1 ovog člana, finansijski subjekt je dužan da: 1) utvrdi sve relevantne IKT sisteme, procese i tehnologije kojima se podržavaju IKT usluge i kritične ili važne funkcije, uključujući i one kojima se podržavaju kritične ili važne funkcije koje obavljaju ili isporučuju treće strane koje pružaju IKT usluge; 2) procijeni koje kritične ili važne funkcije treba da budu obuhvaćene TLPT-om; i 3) u skladu sa procjenom iz tačke 2 ovog stava, precizno definiše planirani obim TLPT-a, kao i da rezultate procjene dostavi nadležnom organu. (7) Nadležni organ prati sve faze pripreme i sprovođenja TLPT-a i odobrava njegove ključne elemente, uključujući i planirani obim TLPT-a iz stava 6 tačka 3 ovog člana, ukoliko procijeni da su ispunjeni uslovi za sprovođenje adekvatnog i efikasnog testiranja.			
3. Ako su treće strane pružatelji IKT usluga obuhvaćene TLPT-om, finansijski 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.	Učešće treće strane koja pruža IKT usluge u TLPT-u Član 30, stav 1 (1) U slučaju kada je treća strana koja pruža IKT usluge obuhvaćena TLPT-om, finansijski subjekt je dužan da preduzme neophodne mjere i zaštitne mehanizme u skladu sa kojima se obezbjeđuje učešće tih trećih strana u TLPT-u, pri čemu ostaje odgovoran za usklađenost sa ovim zakonom.	Potpuno usklađeno		
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, finansijski 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 finansijskog subjekta, skupnog TLPT-a, u kojem sudjeluje više	Član 30, st. 2 do 5 (2) Ako se opravdano može očekivati da će učešće treće strane koja pruža IKT usluge u TLPT-u, u skladu sa stavom 1 ovog člana, negativno uticati na kvalitet ili bezbjednost usluga koje ta treća strana pruža klijentima koji nisu finansijski subjekti iz člana 2 ovog zakona, ili na povjerljivost podataka povezanih sa tim uslugama, finansijski subjekt može sa tom trećom stranom zaključiti sporazum kojim se toj trećoj strani omogućava da direktno zaključi ugovor sa eksternim licem koje vrši testiranje, radi sprovođenja objedinjenog TLPT-a kojim je obuhvaćeno više finansijskih subjekata kojima ta treća strana pruža IKT usluge (u daljem tekstu: objedinjeni TLPT), pod koordinacijom jednog odabranog finansijskog subjekta.	Potpuno usklađeno		

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.	(3) Objedinjeni TLPT mora obuhvatiti relevantan opseg IKT usluga kojima se podržavaju kritične ili važne funkcije koje su financijski subjekti ugovorili sa trećom stranom koja pruža IKT usluge. (4) Ne dovodeći u pitanje zahtjeve iz člana 29 st. 3 i 6 ovog zakona, objedinjeni TLPT se, u smislu člana 29 stav 1 ovog zakona, smatra TLPT-om koji je sproveo financijski subjekt obuhvaćen tim testiranjem. (5) Broj financijskih subjekata koji učestvuju u objedinjenom TLPT-u mora biti prilagođen složenosti i vrsti usluga obuhvaćenih tim testiranjem.			
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.	Član 30, stav 6 (6) Financijski subjekt je dužan da, u suradnji sa trećim stranama koje pružaju IKT usluge, drugim uključenim stranama i licima koja sprovode testiranje, osim nadležnog organa, primijeni efikasne kontrole upravljanja rizicima radi ublažavanja rizika od mogućih negativnih uticaja na podatke, oštećenja imovine i poremećaja u obavljanju kritičnih ili važnih funkcija, usluga i operacija kod samog financijskog subjekta, drugih financijskih subjekata sa kojima ima poslovnu suradnju, kao i u financijskom sektoru.	Potpuno usklađeno		
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.	Izvješćavanje o TLPT-u i međusobna suradnja nadležnih organa u TLPT-u Član 31, stav 1 (1) Po završetku TLPT-a, nakon usaglašavanja izvještaja i planova za otklanjanje utvrđenih nedostataka, financijski subjekt i, kada je to primjenjivo, eksterna lica koja su sprovela TLPT, dužni su da nadležnom organu, odnosno nadležnom organu kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona, dostave rezime relevantnih nalaza, planove za otklanjanje utvrđenih nedostataka i dokumentaciju kojom se potvrđuje da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona.	Potpuno usklađeno		
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.	Član 31, st. 2 do 6 (2) Nadležni organ iz stava 1 ovog člana, financijskom subjektu izdaje potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, kada se to može utvrditi iz dostavljene dokumentacije.	Potpuno usklađeno		

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.	(3) Izuzetno od stava 2 ovog člana, potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, izdaje: 1) nadležni organ koji je vodio TLPT, kada je više nadležnih organa učestvovalo u testiranju; 2) TLPT organ druge države članice, kada je TLPT vodio taj organ. (4) Za potrebe sprovođenja TLPT-a kod finansijskog subjekta koji pruža usluge u više država članica, uključujući i preko filijala, kao i sprovođenja zajedničkog TLPT-a i objedinjenog TLPT-a u slučaju kada treća strana koja pruža IKT usluge pruža IKT usluge finansijskim subjektima u više država članica, nadležni organ sarađuje sa TLPT organima drugih država članica u skladu sa odredbama člana 16 Regulative (EU) br. 2025/1190. (5) U slučaju kada je potvrdu o sprovedenom testiranju izdao organ koji nije zadužen za nadzor finansijskog subjekta, taj finansijski subjekt je dužan da obavijesti svoj nadležni organ o dobijanju te potvrde, i uz obavještenje dostavi rezime relevantnih nalaza i planove za otklanjanje nedostataka. (6) Finansijski subjekt je, i nakon dobijanja potvrde o sprovedenom testiranju, odgovoran za uticaj objedinjenog TLPT-a iz člana 30 stav 2 ovog zakona. Član 8, stav 1, tačka 17 17) TLPT organ druge države članice je: - jedinstveni javni organ u finansijskom sektoru sa sjedištem u drugoj državi članici, koji je imenovan u skladu sa članom 26 stav 9 Regulative (EU) br. 2022/2554; - nadležni organ sa sjedištem u drugoj državi članici kojem je povjereno izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, u skladu sa članom 26 stav 10 Regulative (EU) br. 2022/2554; - nadležni organ iz člana 46 Regulative (EU) br. 2022/2554, sa sjedištem u drugoj državi članici.			
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	Zahtjevi za lica koja su angažovana za sprovođenje TLPT-a Član 32, st. 1 i 2	Djelimično usklađeno	Odredba koja se odnosi na kreditne	Po pristupanju Crne

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.	(1) Financijski subjekt može za potrebe sprovođenja TLPT-a iz člana 29 ovog zakona angažovati interna ili eksterna lica. (2) Financijski subjekt koji za potrebe sprovođenja TLPT-a angažuje interna lica, dužan je da za svako treće sprovođenje TLPT-a angažuje eksterna lica. Član 29 stav 4 (4) Nadležni organ određuje financijske subjekte, koji nisu klasifikovani kao mikro financijski subjekti i nisu subjekti iz člana 21 stav 1 ovog zakona, koji su dužni da sprovode TLPT iz stava 1 ovog člana, uzimajući u obzir princip proporcionalnosti iz člana 5 ovog zakona, na osnovu procjene: 1) uticaja aktivnosti i usluga financijskog subjekta na financijski sektor; 2) mogućih rizika po financijsku stabilnost, uzimajući u obzir sistemski značaj financijskog subjekta na: - nacionalnom nivou; - nivou Evropske unije, kada je to primjenljivo. 3) profila IKT rizika financijskog subjekta, nivoa njegove zrelosti u IKT oblasti i karakteristika tehnologije koju koristi.		institucije koje su u skladu sa članom 6 stav 4 Regulative (EU) br. 1024/2013 klasifikovane kao značajne je neprenosiva jer Crna Gora nije dio SSM-a (Eng. Single Supervisory Mechanism)	Gore EU i nakon što SSM bude prepoznat u posebno m propisu
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.	Nema odgovarajuće odredbe		Opcija nije iskorišćena	
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 zadataka iz ovog članka i članka 27. nekom drugom nacionalnom tijelu u financijskom sektoru.	Član 29 stav 5 (5) Nadležni organ može izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, iz ovog člana i čl. 30 do 32 ovog zakona, da povjeri drugom nadležnom organu, osim određivanja financijskih subjekata koji su dužni da sprovode TLPT.	Potpuno usklađeno		
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;	Nema odgovarajuće odredbe	Neprenosivo		

(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 nacrt 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;	Član 32, stav 3 (3) Angažovana lica za potrebe sprovođenja TLPT-a iz stava 1 ovog člana moraju da: 1) ispunjavaju najviše standarde primjerenosti i ugleda; 2) posjeduju tehničke i organizacione sposobnosti i posebno stručno znanje u oblasti saznanja o prijetnjama, penetracionih testiranja i testiranja crvenog tima; 3) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju u skladu sa zakonom kojim se uređuje postupak	Potpuno usklađeno		

(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 povezanim 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.	akreditacije, ili se pridržavaju formalnih kodeksa ponašanja ili etičkih okvira; 4) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju druge države članice; 5) dostave nezavisno uvjerenje ili revizorski izvještaj kojim se potvrđuje da dobro upravljaju rizicima povezanim sa sprovođenjem TLPT-a, što uključuje adekvatnu zaštitu povjerljivih informacija financijskog subjekta i mehanizme pravne zaštite u pogledu poslovnih rizika financijskog subjekta; 6) koja su propisno i u cijelosti osigurana od profesionalne odgovornosti, uključujući i rizike od protivpravnog 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.	Član 32, stav 4 (4) U slučaju angažovanja internih lica za sprovođenje TLPT-a, financijski subjekt dužan je da obezbijedi da su, pored zahtjeva iz stava 3 ovog člana, ispunjeni i sljedeći zahtjevi: 1) to angažovanje je odobrio nadležni organ, odnosno nadležni organ kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona; 2) nadležni organ je potvrdio da je financijski subjekt obezbijedio dovoljne resurse i preduzeo mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja testiranja; i 3) pružalac saznanja o prijetnjama nije dio financijskog subjekta.	Potpuno usklađeno		
3. Financijski subjekti osiguravaju da se u ugovorima sklopljenima s vanjskim provoditeljima testiranja zahtijeva dobro upravljanje rezultatima TLPT-a i da ni jedna obrada podataka s tim u vezi, uključujući proizvodnju, pohranu, agregiranje, izradu, izvješćivanje, obavješćivanje ili uništavanje, ne stvara rizike za financijski subjekt.	Član 32, stav 5 (5) Financijski subjekt je dužan da obezbijedi da se ugovorom zaključenim sa eksternim licem koje sprovodi TLPT obezbjeđuje dobro upravljanje rezultatima TLPT-a i da bilo kakva obrada podataka u vezi sa tim, uključujući generisanje, izradu, agregiranje, skladištenje, izvješćivanje, saopštavanje i uništavanje podataka, ne stvara rizike za tog financijskog subjekta.	Potpuno usklađeno		
POGLAVLJE V. Upravljanje IKT rizikom povezanim s trećim stranama Odjeljak I. Ključna načela dobrog upravljanja IKT rizikom p ovezanim s trećim stranama	V. UPRAVLJANJE IKT RIZIKOM POVEZANIM SA TREĆIM STRANAMA Ključna načela dobrog upravljanja IKT rizikom povezanim sa trećim stranama Član 33, stav 1	Potpuno usklađeno		

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 proizilaze 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.	(1) Financijski subjekt je dužan da upravlja IKT rizikom povezanim sa trećim stranama kao sastavnim dijelom IKT rizika, u okviru sistema upravljanja IKT rizicima iz člana 10 ovog zakona, u skladu sa sljedećim principima: 1) financijski subjekt koji je zaključio ugovor o korišćenju IKT usluga radi obavljanja svojih poslovnih aktivnosti, u svakom trenutku snosi punu odgovornost za usklađenost sa ovim zakonom i propisima kojima se uređuje poslovanje tog financijskog subjekta; 2) financijski subjekt upravlja IKT rizikom povezanim sa trećim stranama u skladu sa principom proporcionalnosti, uzimajući u obzir: - prirodu, obim, složenost i značaj zavisnosti u oblasti IKT-a; - rizike koji proizilaze iz ugovora o korišćenju IKT usluga zaključenih sa trećim stranama koje pružaju IKT usluge, uzimajući u obzir kritičnost ili značaj konkretne usluge, procesa ili funkcije i potencijalni uticaj na kontinuitet i dostupnost financijskih usluga i aktivnosti, na pojedinačnom nivou i na nivou 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.	Član 33, st. 2 do 4 (2) Financijski subjekt, koji nije klasifikovan kao mikro financijski subjekt i nije subjekt iz člana 21 stav 1 ovog zakona, dužan je da usvoji i redovno preispituje strategiju upravljanja IKT rizikom povezanim sa trećim stranama, uzimajući u obzir strategiju IKT nabavke od više dobavljača iz člana 12 stav 3 ovog zakona, kada je to primjenljivo. (3) Strategija iz stava 2 ovog člana obuhvata politiku korišćenja IKT usluga koje pružaju treće strane za podršku kritičnih ili važnih funkcija financijskog subjekta, i primjenjuje se na pojedinačnoj i, kada je to primjenjivo, na potkonsolidovanoj i konsolidovanoj osnovi. (4) Organ upravljanja financijskog subjekta dužan je da, na osnovu procjene ukupnog rizičnog profila financijskog subjekta, obima i složenosti poslovnih usluga, redovno preispituje rizike	Potpuno usklađeno		

	identifikovane u vezi sa ugovorima o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije.			
3. U sklopu okvira za upravljanje IKT rizicima finansijski 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. Finansijski 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. Finansijski 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 finansijskim subjektom. Finansijski 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.	Registar informacija o ugovorima o korišćenju IKT uslugama i obavješćavanje nadležnog organa Član 34 (1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na pojedinačnoj, kao i na potkonsolidovanoj i konsolidovanoj osnovi, vodi i ažurira registar informacija o svim ugovorima o korišćenju IKT usluga koje pružaju treće strane. (2) Informacije o ugovorima iz stava 1 ovog člana moraju biti evidentirane tako da se ugovori koji se odnose na IKT usluge za podršku kritičnih ili važnih funkcija razlikuju od ugovora koji se ne odnose na te funkcije. (3) Finansijski subjekt je dužan da najmanje jednom godišnje dostavi nadležnom organu izvještaj o broju novih ugovora o korišćenju IKT usluga, kategorijama trećih strana koje pružaju IKT usluge, vrsti ugovora i IKT uslugama i funkcijama koje se pružaju. (4) Finansijski subjekt je dužan da nadležnom organu, na njegov zahtjev, stavi na raspolaganje pojedine dijelove ili cjelokupan registar informacija iz stava 1 ovog člana, uključujući i druge informacije koje su nadležnom organu potrebne za sprovođenje nadzora. (5) Finansijski subjekt je dužan da blagovremeno obavijesti nadležni organ o svakom planiranom ugovoru u skladu sa kojim namjerava da koristi IKT usluge za podršku kritičnih ili važnih funkcija, kao i o svakoj funkciji koja je podržana ugovorom o korišćenju IKT usluga, a koja postane kritična ili važna funkcija.	Potpuno usklađeno		
4. Prije sklapanja ugovornog aranžmana o upotrebi IKT usluga finansijski 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	Član 33, stav 5 (5) Prije zaključenja ugovora o korišćenju IKT usluga, finansijski subjekt je dužan da: 1) procijeni da li se ugovorom predviđa korišćenje IKT usluga koje podržavaju kritične ili važne funkcije; 2) provjeri da li su ispunjeni zahtjevi nadležnog organa za zaključenje ugovora;	Potpuno usklađeno		

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.	3) identifikuje i procijeni sve relevantne rizike povezane sa ugovorom, uključujući i mogućnost da ugovor doprinese povećanju rizika IKT koncentracije iz člana 37 ovog zakona; 4) sprovede detaljnu analizu potencijalnih trećih strana koje pružaju IKT usluge i, kroz postupak odabira i procjene, obezbijedi da je odabrana treća strana adekvatna za pružanje tih usluga; 5) identifikuje i procijeni sukobe interesa koje bi taj ugovor mogao da izazove.			
5. Finansijski 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, finansijski subjekti prije njihova sklapanja propisno vode računa o tome da treće strane pružatelji IKT uslugaprimjenjuju najnovije i najkvalitetnije standarde informacijske sigurnosti.	Standardi bezbjednosti i revizije treće strane koja pruža IKT usluge Član 35, st. 1 i 2 (1) Finansijski subjekt može da zaključi ugovor sa trećom stranom koja pruža IKT usluge, ukoliko ta treća strana primjenjuje odgovarajuće standarde informacione bezbjednosti. (2) U slučaju kada se ugovor iz stava 1 ovog člana odnosi na usluge kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da, prije zaključenja tog ugovora, utvrdi da treća strana koja pruža IKT usluge primjenjuje najnovije i najviše standarde informacione bezbjednosti.	Potpuno usklađeno		
6. Pri ostvarivanju prava na pristup, inspekcijski nadzor i reviziju u odnosu na treću stranu pružatelja IKT usluga finansijski 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, finansijski 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.	Član 35, st. 3 i 4 (3) Radi ostvarivanja prava pristupa, sprovođenja provjera i revizija nad trećom stranom koja pruža IKT usluge, finansijski subjekt dužan je da, primjenom pristupa zasnovanog na procjeni rizika, unaprijed odredi učestalost provjera i revizija, kao i oblasti u kojima će se sprovesti, u skladu sa općeprihvaćenim revizorskim standardima i, kada je to primjenljivo, zahtjevima nadležnog organa u pogledu primjene tih standarda. (4) U slučaju da ugovor zaključen sa trećom stranom koja pruža IKT usluge iz stava 1 ovog člana obuhvata korišćenje IKT usluga koje podrazumijevaju visok stepen tehničke složenosti, finansijski subjekt je dužan da provjeri da li revizori, bilo da su interni, eksterni ili grupa revizora, posjeduju odgovarajuće vještine i znanja neophodna za efikasno sprovođenje relevantnih revizija i procjena.	Potpuno usklađeno		
7. Finansijski subjekti osiguravaju mogućnost raskida ugovornog aranžmana o upotrebi IKT usluga u bilo kojoj od sljedećih situacija:	Raskid ugovora i izlazne strategije Član 36, stav 1	Potpuno usklađeno		

(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 podacima ili pak neosobnim podacima; (d) nadležno tijelo zbog uvjeta dotičnog ugovornog aranžmana ili okolnosti povezanih s dotičnim ugovornim aranžmanom više ne može djelotvorno nadzirati financijski subjekt.	(1) Financijski subjekt je dužan da obezbijedi da se ugovor o korišćenju IKT usluga može raskinuti u sljedećim slučajevima: 1) treća strana koja pruža IKT uslugu značajno je prekršila zakon, propis ili ugovorne obaveze; 2) praćenjem IKT rizika povezanog sa trećom stranom utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjene u izvršavanju funkcija koje se pružaju na osnovu ugovora, uključujući bitne promjene koje utiču na ugovorni odnos ili stanje treće strane koja pruža IKT usluge; 3) treća strana koja pruža IKT usluge je pokazala slabosti u pogledu upravljanja ukupnim IKT rizikom, a naročito u načinu na koji obezbjeđuje dostupnost, autentičnost, integritet i povjerljivost podataka, bez obzira da se radi o podacima o ličnosti, osjetljivim ili drugim podacima; 4) nadležni organ više nije u mogućnosti da sprovodi efikasan nadzor financijskog subjekta zbog uslova ili okolnosti koje se tiču ugovornog odnosa.			
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.	Član 36, st. 2 do 7 (2) Financijski subjekt je dužan da utvrdi izlazne strategije za IKT usluge koje podržavaju kritične ili važne funkcije. (3) Izlaznim strategijama iz stava 2 ovog člana moraju se uzeti u obzir rizici koji mogu nastati na nivou trećih strana koje pružaju IKT usluge, a naročito mogućnost propasti tih trećih strana, pogoršanje kvaliteta IKT usluga koje se pružaju, poremećaji u poslovanju uslijed neadekvatnog ili neuspješnog pružanja IKT usluga, bilo koji značajan rizik koji se odnosi na adekvatnost i kontinuitet pružanja konkretne usluge, kao i mogućnost raskida ugovora sa trećom stranom koja pruža IKT usluge u slučaju iz stava 1 ovog člana. (4) Financijski subjekt je dužan da obezbijedi da raskid ugovora o korišćenju IKT usluga ne dovede do: 1) poremećaja poslovnih aktivnosti tog financijskog subjekta; 2) ograničavanja usklađenosti sa regulatornim zahtjevima; 3) narušavanja kontinuiteta i kvaliteta usluga koje se pružaju klijentima.	Potpuno usklađeno		

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.	(5) Planovi za raskid ugovornih odnosa iz stava 1 ovog člana moraju biti sveobuhvatni, dokumentovani i moraju se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, dovoljno testirati i periodično preispitivati. (6) Finansijski subjekt je dužan da utvrdi alternativna rješenja i razvije tranzicione planove koji mu omogućavaju da, na siguran i cjelovit način, prenese ugovorene IKT usluge i povezane podatke sa treće strane koja pruža IKT usluge na alternativne pružaoce usluga ili ih reintegriše u okviru sopstvenih kapaciteta, kao i da obezbijedi njihovo uklanjanje kod treće strane koja je pružala IKT usluge. (7) Finansijski subjekt je dužan da uspostavi odgovarajuće mjere za nepredviđene situacije radi očuvanja kontinuiteta poslovanja u slučaju nastanka okolnosti iz stava 3 ovog člana.			
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		

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 rizika 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,				
Procjena rizika IKT koncentracije na nivou finansijskog subjekta Član 37, st. 1 i 2 (1) Prilikom identifikacije i procjene rizika iz člana 33 stav 5 točka 3 ovog zakona, finansijski subjekt je dužan da uzme u obzir da li bi zaključivanje ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije dovelo do: 1) angažovanja treće strane koja pruža IKT uslugu koja se ne može lako zamijeniti; ili 2) postojanja više ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije sa istom trećom stranom koja pruža IKT usluge ili sa usko povezanim trećim stranama koje pružaju IKT usluge. (2) Finansijski subjekt je dužan da procijeni prednosti i troškove alternativnih rješenja, kao što je angažman različitih trećih strana koje pružaju IKT usluge, uzimajući u obzir da li i na koji način predviđena rješenja odgovaraju poslovnim potrebama i ciljevima utvrđenim u strategiji digitalne operativne otpornosti tog finansijskog subjekta.		Potpuno usklađeno		
Član 37, st. 3 do 6 (3) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđeno da treća strana koja pruža IKT uslugu, radi pružanja tih usluga, može kao podizvođače angažovati druge pružaoce IKT usluga, finansijski subjekt je dužan da procijeni prednosti i rizike koji mogu proizaći iz tog angažovanja, naročito u slučaju angažovanja IKT podizvođača sa sjedištem u trećoj zemlji. (4) U slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da razmotri propise koji bi se primjenjivali u slučaju insolventnosti treće strane koja pruža IKT usluge, uključujući stečaj i likvidaciju, kao i sva		Potpuno usklađeno		

kao i o svim ograničenjima do kojih bi moglo doći pri hitnom oporavku podataka finansijskog 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, finansijski 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, finansijski 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 finansijskim subjektom.	ograničenja koja bi mogla nastati u slučaju potrebe za hitnim povratkom podataka finansijskog subjekta. (5) U slučaju da se ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije zaključuje sa trećom stranom koja pruža IKT usluge sa sjedištem u trećoj zemlji, finansijski subjekt je dužan da, pored elemenata iz stava 4 ovog člana, razmotri i usklađenost sa odredbama propisa kojima se uređuje zaštita podataka, kao i mogućnost sprovođenja zakona u toj trećoj zemlji. (6) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđena mogućnost angažovanja podizvođača, finansijski subjekt je dužan da procijeni da li, i na koji način, potencijalno dugi ili složeni lanci podugovaranja mogu uticati na njegovu sposobnost da u potpunosti prati ugovorene funkcije, kao i na mogućnost nadležnog organa da sprovodi efikasan nadzor tog finansijskog subjekta.			
Članak 30. Ključne ugovorne odredbe 1. Prava i obaveze finansijskog 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 papirnom obliku ili u dokumentu u nekom drugom trajnom i pristupačnom formatu koji se može preuzeti.	Ključne ugovorne odredbe Član 38, st. 1 i 2 (1) Prava i obaveze finansijskog subjekta i treće strane koja pruža IKT usluge moraju biti uređene ugovorom. (2) Ugovor iz stava 1 ovog člana sadrži i sporazume o nivou usluga, i mora biti dostupan ugovornim stranama u papirnom ili elektronskom obliku koji se može preuzeti u pristupačnom i trajnom formatu.	Potpuno usklađeno		
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 podaci, uključujući lokaciju pohrane, kao i zahtjev da treća strana pružatelj IKT usluga unaprijed obavijesti finansijski subjekt ako namjerava promijeniti takve lokacije;	Član 38, stav 3 (3) Ugovor o korišćenju IKT usluga mora da sadrži: 1) jasan i potpun opis svih funkcija i IKT usluga koje će pružati treća strana koja pruža IKT usluge; 2) odredbe da li treća strana koja pruža IKT usluge može angažovati podizvođače radi pružanja IKT usluge kojom se podržava kritična ili važna funkcija, ili radi pružanja njenih bitnih dijelova, i pod kojim uslovima; 3) lokacije, odnosno regije ili države, sa kojih će se pružati ugovorene i, kada je to primjenljivo, podugovorene funkcije i IKT usluge, kao i lokacije na kojima će se obrađivati podaci, uključujući lokacije na kojima će se skladištiti podaci;	Potpuno usklađeno		

(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 podacima 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.	4) obavezu treće strane koja pruža IKT usluge da unaprijed obavijesti financijski subjekt o namjeri promjene lokacija iz tačke 3 ovog stava; 5) odredbe o zaštiti dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, uključujući podatke o ličnosti; 6) odredbe kojima se financijskom subjektu obezbjeđuje mogućnost pristupa, obnove i povratka podataka o ličnosti i drugih podataka u slučaju insolventnosti, sanacije ili prestanka poslovanja treće strane koja pruža IKT usluge, kao i u slučaju raskida ugovora; 7) opise nivoa usluga, uključujući njihova ažuriranja, odnosno izmjene; 8) obavezu treće strane koja pruža IKT usluge da pruži pomoć financijskom subjektu bez dodatne naknade ili po unaprijed utvrđenoj cijeni, u slučaju IKT incidenta koji je povezan sa IKT uslugom koju ta treća strana pruža financijskom subjektu; 9) obavezu treće strane koja pruža IKT usluge da u suradnje sa nadležnim organom i organom koji je zadužen za sanaciju financijskog subjekta u skladu sa zakonom kojim se uređuje sanacija financijskog subjekta, uključujući i saradnju sa licima koja ovlaste ti organi; 10) prava i uslove za raskid ugovora, sa rokovima za dostavljanje obavještenja o namjeri raskida ugovora, u skladu sa zahtjevima organa iz tačke 9 ovog stava; 11) uslove za učešće treće strane koja pruža IKT usluge u programima za podizanje svijesti o IKT bezbjednosti i obukama o digitalnoj operativnoj otpornosti u skladu sa odredbama člana 19 stav 12 ovog zakona.			
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	Član 38, st. 4 i 5 (4) Ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije mora, pored elemenata iz stava 3 ovog člana, da sadrži: 1) detaljan opis nivoa usluga, uključujući njihova ažuriranja i izmjene, sa preciznim kvantitativnim i kvalitativnim ciljevima učinka u okviru dogovorenih nivoa usluga, kako bi se financijskom	Potpuno usklađeno		

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, inspeksijski 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 inspeksijskih 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 inspeksijskih nadzora i revizija;	subjektu omogućilo efikasno praćenje IKT usluga i preduzimanje, bez odlaganja, odgovarajućih korektivnih mjera u slučaju da dogovoreni nivoi usluga nisu ispunjeni; 2) obavezu treće strane koja pruža IKT usluge da financijskom subjektu dostavlja obavještenja i izvještaje, sa rokovima za njihovo dostavljanje, uključujući i obavještenja o svim okolnostima koje bitno utiču ili bi mogle bitno uticati na sposobnost treće strane koja pruža IKT usluge da efikasno pruža IKT usluge kojima se podržavaju kritične ili važne funkcije, u skladu sa dogovorenim nivoima usluga; 3) zahtjeve koje treća strana koja pruža IKT usluge mora ispunjavati u pogledu primjene i testiranja planova za nepredviđene okolnosti, kao i primjene IKT bezbjednosnih mjera, alata i politika kojima se obezbjeđuje adekvatan nivo bezbjednosti, potreban financijskom subjektu za pružanje usluga u skladu sa zakonom; 4) obavezu treće strane koja pruža IKT usluge da učestvuje u TLPT-u financijskog subjekta i bude maksimalno kooperativna tokom njegovog sprovođenja, u skladu sa odredbama čl. 29 do 32 ovog zakona; 5) pravo kontinuiranog praćenja učinka treće strane koja pruža IKT usluge, što obuhvata: - neograničena prava financijskog subjekta, treće strane koju je ovlastio financijski subjekt i nadležnog organa na pristup, sprovođenje provjera, reviziju, odnosno nadzor nad i kod treće strane koja pruža IKT usluge, kao i pravo na dobijanje kopija relevantne dokumentacije treće strane koja pruža IKT usluge, tako da se ostvarivanje tih prava ne može isključiti ili ograničiti drugim ugovorima ili politikama; - pravo da se, u slučaju kada bi ostvarivanje prava iz alineje 1 ove tačke moglo ugroziti prava drugih klijenata treće strane koja pruža IKT usluge, dogovore alternativni načini provjere učinka treće strane koja pruža IKT usluge, kojima se obezbjeđuje razuman nivo uvjerenja o kvalitetu i bezbjednosti pruženih usluga;	
--	--	--

(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 složenosti 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.	- obavezu treće strane koja pruža IKT usluge da u potpunosti sarađuje tokom neposrednih provjera, revizija i nadzora koje sprovodi nadležni organ, financijski subjekt ili treća strana koju je ovlastio financijski subjekt; - obavezu treće strane koja pruža IKT usluge da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, tokom nadzora koji sprovodi taj organ; - obavezu dostavljanja informacija potrebnih za određivanje obima, procedura koje će se primjenjivati i učestalosti provjera, revizija i nadzora iz al. 3 i 4 ove tačke. 6) odredbe neophodne za realizaciju izlazne strategije, naročito obavezni i adekvatni tranzicioni period: - tokom kojeg će treća strana koja pruža IKT usluge nastaviti pružanje relevantnih funkcija i IKT usluga, radi ublažavanja rizika od nastanka poremećaja kod financijskog subjekta ili radi obezbjeđivanja njegove efikasne sanacije i restrukturiranja; - tokom kojeg financijski subjekt može zamijeniti treću stranu koja pruža IKT usluge ili reintegrirati IKT usluge u okviru sopstvenih kapaciteta, u skladu sa složenosti tih usluga. (5) Izuzetno od stava 4 tačka 5 ovog člana, financijski subjekt koji je klasifikovan kao mikro financijski subjekt može ugovoriti sa trećom stranom koja pruža IKT usluge da se pravo tog financijskog subjekta na pristup, sprovođenje provjera i reviziju nad i kod treće strane koja pruža IKT usluge može povjeriti nezavisnoj trećoj strani, koju odredi treća strana koja pruža IKT usluge, u kom slučaju financijski subjekt od nezavisne treće strane, u svakom trenutku, može zahtijevati informacije i potvrde o učinku treće strane koja pruža IKT usluge.			
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.	Član 38, stav 6 (6) Prilikom usaglašavanja odredbi ugovora sa trećom stranom koja pruža IKT usluge, financijski subjekt je dužan da razmotri primjenu standardizovanih ugovornih klauzula koje su javni organi razvili za određene usluge.	Potpuno usklađeno		
5. Europska nadzorna tijela u okviru Zajedničkog odbora izrađuju nacrt regulatornih tehničkih standarda kojima se preciznije	Nema odgovarajuće odredbe	Neprenosivo		

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 nacrt 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.	Saradnja sa organima Evropske unije i organima trećih država Član 45, stav 6 (6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlaštenja glavnog nadzornog organa u pogledu sprovođenja nadzora.	Potpuno usklađeno		
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:	Nema odgovarajuće odredbe	Neprenosivo		

(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 oslanjaju 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.	Nema odgovarajuće odredbe	Neprenosivo		
4. Ključne treće strane pružatelj 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.	Nema odgovarajuće odredbe	Neprenosivo		
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 podlijezati 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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
7. Imenovanje iz stavka 1. točke (a) ne smije se primjenjivati dok Komisija ne donese delegirani akt u skladu sa stavkom 6.	Nema odgovarajuće odredbe	Neprenosivo		
8. Imenovanje iz stavka 1. točke (a) ne primjenjuje se na: i. financijske subjekte koji pružaju IKT usluge drugim financijskim subjektima;	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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;	Nema odgovarajuće odredbe	Neprenosivo		

(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 imenovala države članice koji su članovi osoblja relevantnog nadležnog tijela.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
8. Zahtjevima utvrđenima u ovom odjeljku ne dovodi se u pitanje primjena Direktive (EU) 2022/2555 i drugih pravila Unije o	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
Članak 33. Zadaci 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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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;	Nema odgovarajuće odredbe	Neprenosivo		

(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 kibernetičkim, i njihovo rješavanje; (f) mehanizme za prenosivost podataka, prenosivost aplikacija i interoperabilnost, kojima se financijskim subjektima osigurava djelotvorno ostvarivanje prava 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 nacrt 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 rizika.	Nema odgovarajuće odredbe	Neprenosivo		
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	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
Članak 35. Ovlašti 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	Nema odgovarajuće odredbe	Neprenosivo		

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 koncentrijskog 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 L 333/58 HR Službeni list Europske unije 27.12.2022. — glavno nadzorno tijelo smatra da primjena takvog podugovaranja predstavlja jasan i ozbiljan rizik za financijsku stabilnost Unije ili za financijske subjekte, što uključuje			
---	--	--	--

spособnost finansijskih subjekata da ispune zahtjeve u pogledu nadzora. Za potrebe podtočke iv. ove točke treće strane pružatelji IKT usluga s pomoću predložka iz članka 41. stavka 1. točke (b) glavnom nadzornom tijelu dostavljaju 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 imenovanim ili uspostavljenim 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.	Nema odgovarajuće odredbe	Neprenosivo		
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 rizika.	Nema odgovarajuće odredbe	Neprenosivo		
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 proslijeđuje izvješća iz stavka 1. točke (c) Zajedničkoj nadzornoj mreži i nadležnim tijelima finansijskih subjekata koji se koriste IKT uslugama te ključne treće strane pružatelja IKT usluga.	Nema odgovarajuće odredbe	Neprenosivo		

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

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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).	Nema odgovarajuće odredbe	Neprenosivo		

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;	Nema odgovarajuće odredbe	Neprenosivo		

(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 izdanim na temelju članka 35. stavka 1. točke (d).	Nema odgovarajuće odredbe	Neprenosivo		
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	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
3. Kad odlukom iz stavka 1. zahtjeva 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.	Nema odgovarajuće odredbe	Neprenosivo		
4. Predstavnici ključnih trećih strana pružatelja IKT usluga dostavljaju tražene informacije. Propisno ovlašteni odvjetnici mogu dostaviti informacije u ime svojih klijenata. Ključna treća	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
3. Službenici i druge osobe koje glavno nadzorno tijelo ovlasti za potrebe istrage iz stavka 1. izvršavaju svoje ovlasti uz predložene 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	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
Članak 39. Inspeksijski 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 inspeksijski nadzor. Za potrebe izvršavanja ovlasti iz prvog podstavka glavno nadzorno tijelo savjetuje se sa Zajedničkom nadzornom mrežom.	Nema odgovarajuće odredbe	Neprenosivo		
2. Službenici i druge osobe koje je glavno nadzorno tijelo ovlastilo za provođenje izravnog inspeksijskog 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 inspeksijskog nadzora i u mjeri u kojoj je to potrebno za inspeksijski nadzor. Službenici i druge osobe koje je ovlastilo glavno nadzorno tijelo izvršavaju svoje ovlasti uz predloženo pisanog ovlaštenja u kojem	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		
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.	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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“).	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		
Članak 41. Usklađivanje uvjeta koji omogućuju provedbu aktivnosti nadzora	Nema odgovarajuće odredbe	Neprenosivo		

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.	Nema odgovarajuće odredbe	Neprenosivo		
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 pružatelj 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 proslijeđuje nadležnim tijelima zaduženima za dotične financijske subjekte.	Nema odgovarajuće odredbe	Neprimjenjivo		
2. Glavno nadzorno tijelo javno obavješćuje o slučajevima u kojima ga ključna treća strana pružatelj IKT usluga ne obavijesti u	Nema odgovarajuće odredbe	Neprimjenjivo		

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 osvijestivosti, 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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		

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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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;	Nema odgovarajuće odredbe	Neprimjenjivo		

(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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Nema odgovarajuće odredbe	Neprimjenjivo		
11. Glavno nadzorno tijelo može na zahtjev pružiti dodatna pojašnjenja o preporukama izdanima radi usmjeravanja nadležnih tijela u pogledu daljnjih mjera.	Nema odgovarajuće odredbe	Neprimjenjivo		
Članak 43. Naknade za nadzor	Nema odgovarajuće odredbe	Neprimjenjivo		

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 razmjeren 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.	Nema odgovarajuće odredbe	Neprimjenjivo		
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.	Saradnja sa organima Evropske unije i organima trećih država Član 45, st. 1 i 2 (1) Nadležni organ može, u cilju jačanja saradnje u oblasti upravljanja IKT rizicima koji se odnose na angažovanje trećih strana, zaključivati sporazume sa nadzornim i regulatornim organima Evropske unije i trećih država. (2) Sporazumi iz stava 1 ovog člana mogu obuhvatati razmjenu iskustava i primjera dobre prakse, saradnju u preispitivanju okvira upravljanja IKT rizicima, mjera za njihovo ublažavanje, kao i razmjenu informacija u vezi sa postupanjem u slučaju IKT incidenata.	Potpuno usklađeno		
	Nema odgovarajuće odredbe	Neprenosivo		

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.	VI. RAZMJENA INFORMACIJA Razmjena informacija i saznanja o sajber prijetnjama Član 39, stav 1 (1) Financijski subjekti mogu međusobno razmjenjivati informacije i saznanja o sajber prijetnjama, uključujući indikatore ugroženosti, taktike, tehnike i procedure, bezbjednosna upozorenja i alate za konfiguraciju, u mjeri u kojoj ta razmjena: 1) ima za cilj jačanje digitalne operativne otpornosti financijskih subjekata, naročito podizanjem svijesti o sajber prijetnjama, ograničavanje ili sprečavanje njihovog širenja, unapređenje odbrambenih kapaciteta, tehnika za otkrivanje prijetnji, strategija za ublažavanje uticaja ili postupaka odgovora i oporavka; 2) se sprovodi u okviru pouzdane zajednice financijskih subjekata; 3) se ostvaruje kroz sporazume za razmjenu informacija kojima se štiti potencijalno osjetljiva priroda tih informacija, koji su uređeni pravilima ponašanja kojima se obezbeđuje potpuna zaštita povjerljivih poslovnih informacija, podataka o ličnosti u skladu sa propisom kojim se uređuje zaštita podataka o ličnosti i primjena pravila u oblasti zaštite konkurencije. Član 39, stav 2 (2) Sporazumima za razmjenu informacija iz stava 1 tačka 3 ovog člana moraju se utvrditi uslovi za učešće u razmjeni informacija i, kada je to primjenljivo, učešće i uloga javnih organa koji mogu biti uključeni u tim sporazumima, trećih strana koje pružaju IKT usluge, kao i operativni elementi, uključujući i upotrebu posebnih IT platformi. Član 39, stav 3 (3) Financijski subjekt je dužan da obavijesti nadležni organ bez odlaganja ako je učesnik u sporazumu za razmjenu informacija iz stava 1 tačka 3 ovog člana, odnosno kada prestane sa učešćem u tom sporazumu.	Potpuno usklađeno Potpuno usklađeno Potpuno usklađeno		
--	--	--	--	--

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 kriptovalutama koji imaju odobrenje za rad na temelju Uredbe o tržištima kriptovalutne i izdavalje 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	Nadležni organ Član 3, stav 1 (1) Nadležni organ, u smislu ovog zakona, je organ koji je u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta iz člana 2 stav 1 ovog zakona nadležan za kontrolu, superviziju, odnosno nadzor tog subjekta, i to: 1) za finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona, Centralna banka Crne Gore (u daljem tekstu: Centralna banka); 2) za finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona, Komisija za tržište kapitala Crne Gore (u daljem tekstu: Komisija); 3) za finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona, Agencija za nadzor osiguranja (u daljem tekstu: Agencija); 4) za finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona, organ utvrđen posebnim zakonom.	Djelimično usklađeno	Usklađivanje izvršeno za sve subjekte koji postoje u Crnoj Gori. Odredbe koje se odnose na druge subjekte nisu primjenjive. Odrađen je reg. maksimum, dalje usklađivanje je moguće samo po pristupanju.
---	---	-----------------------------	---

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; (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	Nema odgovarajuće odredbe		Član 14 Direktive 2022/2555 (Grupa za suradnju) nije transponovan u Zakon o informacionoj bezbjednosti	

nađ 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 CSIRTovima imenovanim ili uspostavljenim u skladu s Direktivom (EU) 2022/2555.	VIII. SARADNJA NADLEŽNIH ORGANA SA DRUGIM ORGANIMA Saradnja sa organima iz zakona kojim se uređuje informaciona bezbjednost Član 44, stav 1 (1) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost određen kao jedinstvena nacionalna kontakt tačka za informacionu bezbjednost.	Potpuno usklađeno		
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.	Član 44, st. 2 i 3 (2) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost nadležan za zaštitu finansijskih subjekata od sajber prijetnji i incidenata i od njega može zatražiti relevantnu pomoć. (3) Saradnja iz stava 2 ovog člana uređuje se sporazumima između nadležnih organa i tog organa.	Potpuno usklađeno		
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.	Nema odgovarajuće odredbe		Opcija nije iskorišćena	

Članak 48. Suradnja tijela 1. Nadležna tijela blisko surađuju međusobno i, ako je to primjenljivo, s glavnim nadzornim tijelom.	Član 3, stav 2 (2) Nadležni organi iz stava 1 ovog člana dužni su da međusobno sarađuju i razmjenjuju informacije i podatke potrebne za sprovođenje ovog zakona. Član 45, stav 6 (6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlašćenja glavnog nadzornog organa u pogledu sprovođenja nadzora.	Potpuno usklađeno		
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, pristupa i mjera poduzetih u okviru nadzornih zadaća glavnog nadzornog tijela.	Član 45, stav 6 (6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlašćenja glavnog nadzornog organa u pogledu sprovođenja nadzora.	Potpuno usklađeno		
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	Član 45, stav 7 (7) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om i EIOPA-om i drugim relevantnim organima, u vezi sa učešćem u uspostavljanju mehanizma za razmjenu dobre prakse u cilju unapređenja međusektorske svijesti o stanju i identifikaciji zajedničkih ranjivosti i rizika u oblasti sajber bezbjednosti, uključujući i učešće u razvoju i sprovođenju vježbi za upravljanje kriznim i nepredviđenim situacijama, scenarijima sajber napada i drugih aktivnosti koje doprinose uspostavljanju efikasnog i koordinisanog odgovora na nivou Evropske unije u slučaju značajnih prekograničnih IKT incidenata ili srodnih prijetnji sa sistemskim uticajem na	Potpuno usklađeno	Odredbe koje se direktno odnose na obaveze ESA i drugih EU organa i tijela su neprenosive	

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 kibernetičkih napada, radi razvoja komunikacijskih kanala i postupnog omogućavanja 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.	financijski sektor, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.			
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.	Član 45, st. 1, 2 i 7 (1) Nadležni organ može, u cilju jačanja saradnje u oblasti upravljanja IKT rizicima koji se odnose na angažovanje trećih strana, zaključivati sporazume sa nadzornim i regulatornim organima Evropske unije i trećih država. (2) Sporazumi iz stava 1 ovog člana mogu obuhvatati razmjenu iskustava i primjera dobre prakse, saradnju u preispitivanju okvira upravljanja IKT rizicima, mjera za njihovo ublažavanje, kao i razmjenu informacija u vezi sa postupanjem u slučaju IKT incidenata. (7) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om i EIOPA-om i drugim relevantnim organima, u vezi sa učešćem u uspostavljanju mehanizma za razmjenu dobre prakse u cilju unapređenja međusektorske svijesti o stanju i identifikaciji zajedničkih ranjivosti i rizika u oblasti sajber bezbjednosti, uključujući i učešće u razvoju i sprovođenju vježbi za upravljanje kriznim i nepredviđenim situacijama, scenarijima sajber napada i drugih aktivnosti koje doprinose uspostavljanju efikasnog i koordinisanog odgovora na nivou Evropske unije u slučaju značajnih prekograničnih IKT incidenata ili srodnih prijetnji sa sistemskim uticajem na finansijski sektor, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.	Potpuno usklađeno	Odredbe koje se direktno odnose na obaveze ESA i ECB-a su neprenosive	
Članak 50. Administrativne kazne i korektivne mjere	VII. NADZOR NAD SPROVOĐENJEM ODREDBI OVOG ZAKONA I NADZORNE MJERE Obim nadležnosti	Potpuno usklađeno		

1. Nadležna tijela imaju sve ovlasti nadzora, istrage i sankcioniranja potrebne za izvršavanje svojih zadaća iz ove Uredbe.	Član 40, st. 1, 2 i 3 (1) Nadzor nad sprovođenjem ovog zakona vrši nadležni organ. (2) U sprovođenju nadzora iz stava 1 ovog člana, nadzorni organ: 1) izriče mjere finansijskom subjektu; 2) podnosi predloge za pokretanje prekršajnih postupaka zbog kršenja odredbi ovog zakona. (3) Nadzor iz stava 2 tačka 1 ovog člana sprovodi se u skladu sa ovim zakonom i zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta.			
2. Ovlaсти iz stavka 1. uključuju najmanje sljedeće ovlasti: (a) pristup svim dokumentima ili podacima 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 finansijskih 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.	Obim nadležnosti Član 40, st. 4 (4) U vršenju nadzora iz stava 1 ovog člana, nadležni organ može naročito da: 1) pristupi svim dokumentima ili podacima u bilo kom obliku koje smatra relevantnim za izvršavanje svojih ovlaštenja i pribavi kopije tih dokumenata ili podataka; 2) sprovede neposredni nadzor ili kontrolu, koji uključuju, ali nisu ograničeni na: - ovlaštenje da od finansijskog subjekta i lica zaposlenih u finansijskom subjektu zahtijeva pisana i usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole; - obavljanje razgovora sa bilo kojim fizičkim ili pravnim licem za koje ocijeni da ima relevantna saznanja, uz izričitu saglasnost tog lica, u svrhu prikupljanja informacija koje se odnose na predmet kontrole; 3) zahtijeva sprovođenje korektivnih mjera zbog kršenja odredbi ovog zakona.	Potpuno usklađeno		
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.	Obim nadležnosti Član 40, st. 1, 2 i 3 (1) Nadzor nad sprovođenjem ovog zakona vrši nadležni organ. (2) U sprovođenju nadzora iz stava 1 ovog člana, nadzorni organ: 1) izriče mjere finansijskom subjektu; 2) podnosi predloge za pokretanje prekršajnih postupaka zbog kršenja odredbi ovog zakona.	Potpuno usklađeno		

	(3) Nadzor iz stava 2 tačka 1 ovog člana sprovodi se u skladu sa ovim zakonom i zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta. Način utvrđivanja mjera Član 41 stav 3 (3) Mjere nadležnog organa izrečene u skladu sa odredbama ovog zakona, moraju biti efikasne, srazmjerne 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 finansijske prirode, kako bi se osiguralo da finansijski 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.	Obim nadležnosti Član 40, stav 5 (5) Pored mjera koje je nadležni organ ovlašten da izriče u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, nadležni organ je ovlašten da u vršenju nadzora u skladu sa ovim zakonom: 1) naloži finansijskom subjektu i odgovornom licu u finansijskom subjektu da prekine, postupanje koje predstavlja kršenje ovog zakona i propisa donesenih na osnovu ovog zakona; 2) naloži finansijskom subjektu da privremeno ili trajno prekine sa postupanjem koje nadležni organ smatra kršenjem ovog zakona i propisa donesenih na osnovu ovog zakona i da spriječi ponavljanje takvog postupanja; 3) izrekne kaznu, uključujući i novčanu kaznu, kako bi se obezbijedilo da finansijski subjekt nastavi sa ispunjavanjem zahtjeva iz ovog zakona i propisa donesenih na osnovu ovog zakona; 4) uputi zahtjev, u skladu sa zakonom, za dostavljanje evidencije telekomunikacionog operatera o prometu podataka koji su od značaja za utvrđivanje povreda ovog zakona i propisa donesenih na osnovu ovog zakona, kada postoji opravdana sumnja na takvu povredu; 5) izda javno obavještenje o kršenju zakona, u kojem može da navede identitet finansijskog subjekta koji je bio predmet nadzora, odnosno kontrole, lica u tom finansijskom subjektu odgovorna za kršenje zakona i propisa donesenih na osnovu ovog zakona kao i prirodu tog kršenja.	Potpuno usklađeno		

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.	Obim nadležnosti Član 40, stav 6 (6) Nadležni organ može naložiti finansijskom subjektu da razriješi člana upravnog odbora ili drugo lice sa rukovodeće funkcije u tom finansijskom subjektu kada utvrdi njegovu odgovornost za kršenje ovog zakona.	Potpuno usklađeno		
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.	Obim nadležnosti Član 40, stav 7 (7) Finansijski subjekt kome je naložena mjera iz st. 5 ili 6 ovog člana, dužan je da izvrši tu mjeru na način i u roku utvrđenim rješenjem o izricanju mjere.	Potpuno usklađeno		
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.	Način utvrđivanja mjera Član 41, stav 1 (1) Nadležni organ izvršava ovlaštenje za izricanje mjera iz člana 40 ovog zakona, u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, i to: 1) neposrednim postupanjem; 2) u suradnji sa nadležnim i drugim organima; 3) povjeravanjem pojedinih poslova drugim organima, u okviru sopstvene odgovornosti; ili 4) podnošenjem zahtjeva nadležnom pravosudnom organu.	Potpuno usklađeno		
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) finansijsku 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;	Način utvrđivanja mjera Član 41, stav 2 (2) Prilikom odlučivanja o vrsti i visini mjere iz člana 40 stav 4 ovog zakona, nadležni organ uzima u obzir stepen namjere ili nehat u postupanju kojim je izvršeno kršenje odredbi ovog zakona i propisa donesenih na osnovu ovog zakona kao i sve druge relevantne okolnosti, naročito: 1) značaj, težinu i trajanje kršenja, odnosno ponavljanje ili učestalost kršenja; 2) stepen odgovornosti finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje; 3) finansijsku sposobnost finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje;	Potpuno usklađeno		

(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.	4) iznos stečene dobiti ili izbjegnuto gubitka finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, ako se taj iznos može utvrditi; 5) gubitke trećih lica nastale kršenjem, ako se mogu utvrditi; 6) saradnju finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, sa nadležnim organom, bez prejudiciranja obaveze povraćaja koristi ili izbjegnuto gubitka; 7) prethodna kršenja i izrečene mjere finansijskom subjektu, odnosno fizičkom licu odgovornom za kršenje.			
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.	Nema odgovarajuće odredbe		Opcija nije iskorišćena	
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.	Saradnja u slučaju krivičnog djela Član 42 Nadležni organ je dužan da u okviru svoje nadležnosti sarađuje sa pravosudnim organima i organima nadležnim za sprovođenje krivičnih sankcija radi razmjene informacija potrebnih za vođenje istraga i postupka u vezi sa sprovođenjem sankcija za krivično djelo u oblasti digitalne operativne otpornosti propisano zakonom.	Poptuno usklađeno		
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.	Saradnja sa organima Evropske unije i organima trećih država Član 45, stav 8, tačka 1 (8) Nadležni organ je dužan da obavještava Evropsku komisiju EBA-u, ESMA-u i EIOPA-u o: 1) propisima kojima se bliže uređuju zahtjevi iz ovog zakona, kao i o izmjenama tih propisa u rokovima propisanim Regulativom (EU) 2022/2554;	Potpuno usklađeno		

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.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, stav 1 (1) Nadležni organ na svojoj internet stranici, bez odlaganja, objavljuje podatke o novčanim kaznama izrečenim pravosnažnim rješenjem iz člana 40 stav 4 tačka 3 ovog zakona i pravosnažnim kaznama finansijskom subjektu i odgovornom licu u finansijskom subjektu izrečenim u prekršajnom postupku zbog kršenja odredbi ovog zakona ili propisa donesenih na osnovu ovog zakona.	Potpuno usklađeno		
2. Objava iz stavka 1. uključuje informacije o vrsti i prirodi povrede, identitetu odgovornih osoba te izrečenim kaznama.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, stav 2 (2) Podaci iz stava 1 ovog člana sadrže informacije o vrsti i prirodi kršenja, naziv finansijskog subjekta i ime i prezime odgovornih lica u finansijskom subjektu kome je izrečena kazna.	Potpuno usklađeno		
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 finansijskih 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 finansijskih tržišta ili da takva objava nije razmjerna u odnosu na blagost izrečene kazne.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, stav 3 (3) Izuzetno od st. 1 i 2 ovog člana, ako na pojedinačnoj osnovi nadležni organ procijeni da objavljivanje identiteta finansijskog subjekta ili ličnih podataka odgovornih lica u finansijskom subjektu nije srazmjerno utvrđenom kršenju, ili bi objavljivanje ugrozilo stabilnost finansijskog tržišta, istražne radnje u krivičnom postupku koje su u toku, ili bi objavljivanje prouzrokovalo nesrazmjernu štetu za finansijski subjekt ili odgovorna lica, koju je moguće utvrditi, nadležni organ može da: 1) odloži objavljivanje podataka iz st. 1 i 2 ovog člana do prestanka razloga za neobjavljivanje; 2) izvrši objavljivanje na način kojim se ne oduju podaci iz st. 1 i 2 ovog člana, s tim što se i to objavljivanje može odložiti; 3) ne objavi podatke iz st. 1 i 2 ovog člana ako ocijeni da opcije iz tač. 1 i 2 ovog stava ne mogu u dovoljnoj mjeri obezbijediti	Potpuno usklađeno		

	stabilnost finansijskog tržišta ili da to objavljivanje nije srazmjerno težini 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.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, stav 3, tačka 2 (3) Izuzetno od st. 1 i 2 ovog člana, ako na pojedinačnoj osnovi nadležni organ procijeni da objavljivanje identiteta finansijskog subjekta ili ličnih podataka odgovornih lica u finansijskom subjektu nije srazmjerno utvrđenom kršenju, ili bi objavljivanje ugrozilo stabilnost finansijskog tržišta, istražne radnje u krivičnom postupku koje su u toku, ili bi objavljivanje prouzrokovalo nesrazmjernu štetu za finansijski subjekt ili odgovorna lica, koju je moguće utvrditi, nadležni organ može da: 1) odloži objavljivanje podataka iz st. 1 i 2 ovog člana do prestanka razloga za neobjavljivanje; 2) izvrši objavljivanje na način kojim se ne odaju podaci iz st. 1 i 2 ovog člana, s tim što se i to objavljivanje može odložiti; 3) ne objavi podatke iz st. 1 i 2 ovog člana ako ocijeni da opcije iz tač. 1 i 2 ovog stava ne mogu u dovoljnoj mjeri obezbijediti stabilnost finansijskog tržišta ili da to objavljivanje nije srazmjerno težini izrečene kazne.	Potpuno usklađeno		
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.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, st. 1 i 2 (1) Nadležni organ na svojoj internet stranici, bez odlaganja, objavljuje podatke o novčanim kaznama izrečenim pravosnažnim rješenjem iz člana 40 stav 4 tačka 3 ovog zakona i pravosnažnim kaznama finansijskom subjektu i odgovornom licu u finansijskom subjektu izrečenim u prekršajnom postupku zbog kršenja odredbi ovog zakona ili propisa donesenih na osnovu ovog zakona. (2) Podaci iz stava 1 ovog člana sadrže informacije o vrsti i prirodi kršenja, naziv finansijskog subjekta i ime i prezime odgovornih lica u finansijskom subjektu kome je izrečena kazna.	Potpuno usklađeno		

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.	Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima Član 43, stav 4 (4) Podaci iz st. 1, 2 i 3 ovog člana ostaju na internet stranici nadležnog organa pet godina od dana objavljivanja.	Potpuno usklađeno		
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.	IX. POSLOVNA Tajna i ZAŠTITA PODATAKA O LIČNOSTI Čuvanje poslovne tajne Član 46, stav 1 (1) Sve povjerljive informacije koje nadležni organ primi, razmijeni ili prenese u vezi sa sprovođenjem ovog zakona smatraju se tajnom u skladu sa zakonom i podliježu obavezi čuvanja tajne.	Potpuno usklađeno		
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.	Član 46, stav 2 (2) Obaveza čuvanja poslovne tajne iz stava 1 ovog člana odnosi se na sva lica zaposlena ili angažovana od strane nadležnog organa, kao i sva druga pravna ili fizička lica kojima nadležni organ, u skladu sa zakonom, povjeri obavljanje pojedinih poslova ili ovlašćenja, uključujući revizore i spoljne eksperte.	Potpuno usklađeno		
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;	Član 46, stav 3 (3) Informacije koje predstavljaju poslovnu tajnu ne mogu se saopštavati trećim licima, osim ako je to propisano ovim zakonom ili drugim propisom. (4) Sve informacije koje se razmjenjuju između nadležnih organa u skladu sa ovim zakonom, a koje se odnose na poslovanje finansijskog subjekta ili operativne uslove, ekonomske ili lične, smatraju se povjerljivim, osim ako nadležni organ prilikom dostavljanja informacija izričito ne navede da se iste mogu objavljivati ili ako je njihovo objavljivanje nužno za vođenje sudskog postupka. (5) Obavješćavanje i razmjena podataka između nadležnih organa, odnosno između nadležnih organa i drugih organa u skladu sa ovim zakonom, ne predstavlja kršenje obaveze čuvanja povjerljivih informacija utvrđene posebnim zakonom.	Potpuno usklađeno		
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	Član 46, stav 4 (4) Sve informacije koje se razmjenjuju između nadležnih organa u skladu sa ovim zakonom, a koje se odnose na poslovanje finansijskog	Potpuno usklađeno		

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.	subjekta ili operativne uslove, ekonomske ili lične, smatraju se povjerljivim, osim ako nadležni organ prilikom dostavljanja informacija izričito ne navede da se iste mogu objavljivati ili ako je njihovo objavljivanje nužno za vođenje sudskog postupka. (5) Obavješćavanje i razmjena podataka između nadležnih organa, odnosno između nadležnih organa i drugih organa u skladu sa ovim zakonom, ne predstavlja kršenje obaveze čuvanja povjerljivih informacija utvrđene posebnim zakonom.			
Članak 56. Zaštita podataka 1. Europskim nadzornim tijelima i nadležnim tijelima dopušteno je obrađivati osobne podatke samo ako je to potrebno za izvršavanje njihovih obaveza i zadaća na temelju ove Uredbe, posebno za istragu, inspeksijski 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.	Obrada i zaštita podataka o ličnosti Član 47, st. 1 i 2 (1) Nadležni organ obrađuje podatke o ličnosti samo u mjeri u kojoj je to neophodno za izvršavanje ovlaštenja u skladu sa ovim zakonom, naročito prilikom vršenja nadzora i kontrole, zahtijeva za dostavljanje informacija, komunikacije, objavljivanja informacija, evaluacije, provjere, procjene i izrade planova nadzora. (2) Obrada podataka o ličnosti iz stava 1 ovog člana vrši se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.	Potpuno usklađeno		
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 najduže 15 godina, osim u slučaju sudskih postupaka koji su u tijeku i zahtijevaju da se takvi podatci čuvaju dulje.	Član 47, st. 3 i 4 (3) Podaci o ličnosti iz stava 1 ovog člana mogu se čuvati samo onoliko koliko je potrebno za vršenje ovlaštenja u vezi sa nadzorom finansijskog subjekta, a najduže 15 godina. (4) Izuzetno od stava 3 ovog člana, podaci o ličnosti se mogu čuvati duže u slučaju vođenja sudskih postupaka, odnosno do okončanja postupka.	Potpuno usklađeno		
Članak 57-58	Nema odgovarajuće odredbe	Neprenosivo		
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,	Nema odgovarajuće odredbe		Materija nije predmet regulisanja ovog propisa	

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 (*). 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.-); (b) stavak 6. briše se; 2. članak 34. mijenja se kako slijedi: (a) stavak 1. zamjenjuje se sljedećim:	Nema odgovarajuće odredbe		Materija je predmet regulisanja posebnih propisa iz oblasti tržišta kapitala.	

„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 pojedinačni zahtjevi 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	Nema odgovarajuće odredbe	Materija je predmet regulisanja posebnih propisa iz oblasti tržišta kapitala.
---	----------------------------------	--

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 (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:	Nema odgovarajuće odredbe		Materija je predmet regulisanja posebnih propisa iz oblasti tržišta kapitala.

„(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..).“	Nema odgovarajuće odredbe		Materija je predmet regulisanja posebnih propisa iz oblasti tržišta kapitala.	
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.	Nema odgovarajuće odredbe	Neprenosivo		