I

(Zakonodajni akti)

UREDBE

UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA

z dne 14. decembra 2022

o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropske centralne banke ([1]),

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ([2]),

v skladu z rednim zakonodajnim postopkom ([3]),

ob upoštevanju naslednjega:

(1) V digitalni dobi informacijska in komunikacijska tehnologija (IKT) podpira kompleksne sisteme, ki se uporabljajo za vsakodnevne dejavnosti. Zagotavlja delovanje naših gospodarstev v ključnih sektorjih, vključno s finančnim sektorjem, in krepi delovanje notranjega trga. Z vse večjo digitalizacijo in medsebojno povezanostjo se povečuje tudi tveganje na področju IKT, zaradi česar je družba kot celota – in zlasti finančni sistem – bolj izpostavljena kibernetskim grožnjam ali motnjam na področju IKT. Čeprav so vsesplošna uporaba sistemov IKT ter visoka digitalizacija in povezljivost danes bistvene značilnosti dejavnosti finančnih subjektov v Uniji, je treba njihovo digitalno odpornost bolje obravnavati in jo vgraditi v njihove širše operativne okvire.

(2) Uporaba IKT je v zadnjih desetletjih dobila osrednjo vlogo pri opravljanju finančnih storitev, in sicer do takšne mere, da je danes ključna za delovanje tipičnih dnevnih funkcij v vseh finančnih subjektih. Digitalizacija zdaj zajema na primer plačila, ki so se z gotovinskih in papirnatih metod vse bolj preusmerila v uporabo digitalnih rešitev, ter kliring in poravnave vrednostnih papirjev, elektronsko in algoritemsko trgovanje, posli posojanja in financiranja, medsebojno financiranje, bonitetne ocene, obravnavo zahtevkov in operacije zalednih služb. Tudi zavarovalniški sektor se je spremenil z uporabo IKT, in sicer od pojava zavarovalnih posrednikov, ki ponujajo svoje storitve prek

([1]) UL C 343, 26.8.2021, str. 1.
([2]) UL C 155, 30.4.2021, str. 38.
([3]) Stališče Evropskega parlamenta z dne 10. novembra 2022 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 28. novembra 2022.

spleta in uporabljajo zavarovalniško tehnologijo, do digitalnega sklepanja zavarovanj. Finance so postale večinoma digitalne v celotnem sektorju, poleg tega pa je digitalizacija poglobila medsebojne povezave in odvisnosti znotraj samega finančnega sektorja ter v odnosu do infrastrukture tretjih strani in tretjih ponudnikov storitev.

(3) Evropski odbor za sistemska tveganja (ESRB) je v poročilu iz leta 2020, ki obravnava sistemska kibernetska tveganja, ponovno potrdil, da lahko obstoječa visoka stopnja medsebojne povezanosti finančnih subjektov, finančnih trgov in infrastruktur finančnega trga ter zlasti medsebojna odvisnost njihovih sistemov IKT, predstavlja sistemsko ranljivost, ker bi se lahko lokalizirani kibernetski incidenti iz katerega koli od približno 22 000 finančnih subjektov v Uniji hitro razširili na celotni finančni sistem, ne da bi jih pri tem ovirale geografske meje. Resne kršitve na področju IKT, do katerih prihaja v finančnem sektorju, ne vplivajo le na posamezne finančne subjekte. Omogočajo tudi, da se lokalizirane ranljivosti širijo po transmisijskih kanalih finančnega sistema in lahko povzročijo škodljive posledice za stabilnost finančnega sistema Unije, kot sta upad likvidnosti in splošna izguba zaupanja v finančne trge.

(4) V zadnjih letih je tveganje na področju IKT pritegnilo pozornost oblikovalcev politik, regulativnih organov in organov za določanje standardov, in sicer na mednarodni, na ravni Unije in na nacionalni ravni, ki skušajo povečati digitalno odpornost, določiti standarde ter uskladiti regulativno ali nadzorniško delo. Na mednarodni ravni Baselski odbor za bančni nadzor, Odbor za plačila in tržno infrastrukturo, Odbor za finančno stabilnost, Inštitut za finančno stabilnost ter G7 in G20 delujejo z namenom pristojnim organom in upravljavcem trga v različnih jurisdikcijah zagotoviti orodja za krepitev odpornosti njihovih finančnih sistemov. To delo temelji tudi na potrebi po ustreznem upoštevanju tveganja na področju IKT v kontekstu medsebojno zelo povezanega svetovnega finančnega sistema in prizadevanju za večjo usklajenost zadevnih najboljših praks.

(5) Kljub ciljno usmerjenim političnim in zakonodajnim pobudam na ravni Unije in nacionalni ravni tveganje na področju IKT še naprej predstavlja izziv za operativno odpornost, uspešnost in stabilnost finančnega sistema Unije. Reforme, ki so sledile finančni krizi leta 2008, so predvsem okrepile finančno odpornost finančnega sektorja Unije ter si prizadevale zaščititi konkurenčnost in stabilnost Unije z vidika gospodarstva, bonitetnega vidika in vidika ravnanja na trgu. Čeprav sta varnost IKT in digitalna odpornost del operativnega tveganja, nista bili v središču regulativnega programa po finančni krizi in sta se razvili le na nekaterih področjih politike finančnih storitev in regulativne ureditve Unije ali le v nekaj državah članicah.

(6) Komisija je v sporočilu z dne 8. marca 2018 z naslovom „Akcijski načrt za finančno tehnologijo: za bolj konkurenčen in inovativen evropski finančni sektor" poudarila, da je izjemno pomembno povečati odpornost finančnega sektorja Unije, vključno z operativnega vidika, da se zagotovi njegova tehnološka varnost in dobro delovanje ter hitro okrevanje po kršitvah in incidentih na področju IKT, kar bi nazadnje omogočilo učinkovito in nemoteno opravljanje finančnih storitev po vsej Uniji, tudi v stresnih situacijah, ter hkrati ohranjalo zaupanje potrošnikov in trga.

(7) Aprila 2019 so Evropski nadzorni organ (Evropski bančni organ), (EBA), ustanovljen z Uredbo (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([4]), Evropski nadzorni organ (Evropski organ za zavarovanja in poklicne pokojnine), (EIOPA), ustanovljen z Uredbo (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([5]), in Evropski nadzorni organ (Evropski organ za vrednostne papirje in trge) (ESMA), ustanovljen z Uredbo (EU) št. 1095/2010

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

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

Evropskega parlamenta in Sveta ([6]), (v nadaljnjem besedilu skupaj znani kot: evropski nadzorni organi) skupaj izdali tehnični nasvet in pozvali k doslednemu pristopu k tveganju na področju IKT v finančnem sektorju ter priporočili, naj se s sektorsko pobudo Unije na sorazmeren način okrepi digitalna operativna odpornost industrije finančnih storitev.

(8) Finančni sektor Unije urejajo enotna pravila, upravlja pa ga Evropski sistem finančnega nadzora. Vendar določbe o digitalni operativni odpornosti in varnosti IKT še niso v celoti ali dosledno harmonizirane, čeprav je digitalna operativna odpornost ključna za zagotavljanje finančne stabilnosti in celovitosti trga v digitalni dobi in nič manj pomembna kot na primer skupni bonitetni standardi ali standardi ravnanja na trgu. Zato bi bilo treba enotna pravila in sistem nadzora oblikovati tako, da bi zajemala tudi digitalno operativno odpornost, in sicer z okrepitvijo pooblastil pristojnih organov, da se jim omogoči nadzor nad obvladovanjem tveganj na področju IKT v finančnem sektorju, da bi se zavarovali celovitost in učinkovitost notranjega trga ter olajšalo njegovo pravilno delovanje.

(9) Zakonodajne razlike in neenakomerni nacionalni regulativni ali nadzorni pristopi v zvezi s tveganjem na področju IKT ovirajo delovanje notranjega trga finančnih storitev, kar omejuje nemoteno uveljavljanje svobode ustanavljanja in opravljanje storitev za finančne subjekte, ki poslujejo čezmejni podlagi. Izkrivljena bi lahko bila tudi konkurenca med finančnimi subjekti iste vrste, ki poslujejo v različnih državah članicah. To velja zlasti za področja, na katerih je bila harmonizacija na ravni Unije zelo omejena, kot na primer pri testiranju digitalne operativne odpornosti, ali pa harmonizacije sploh ni, kot na primer pri spremljanju tveganja tretjih strani na področju IKT. Razlike, ki izhajajo iz razvoja, predvidenega na nacionalni ravni, bi lahko povzročile dodatne ovire za delovanje notranjega trga v škodo udeležencev na trgu in finančne stabilnosti.

(10) Ker so bile določbe, povezane s tveganjem na področju IKT, na ravni Unije do zdaj obravnavne le delno, obstajajo vrzeli ali prekrivanja na pomembnih področjih, kot sta poročanje o incidentih, povezanih z IKT, in testiranje digitalne operativne odpornosti, ter neskladja, ki so posledica nastajajočih različnih nacionalnih pravil ali stroškovno neučinkovite uporabe prekrivajočih se pravil. To je zlasti škodljivo za intenzivne uporabnike IKT, kot je finančni sektor, saj tehnološka tveganja nimajo meja, finančni sektor pa svoje storitve zagotavlja na široki čezmejni podlagi znotraj in zunaj Unije. Posamezni finančni subjekti, ki poslujejo na čezmejni podlagi ali imajo več dovoljenj (npr. en finančni subjekt ima lahko dovoljenje za opravljanje bančnih storitev, dovoljenje za investicijsko podjetje in dovoljenje za plačilno institucijo, pri čemer je vsako dovoljenje izdal drug pristojni organ v eni ali več državah članicah), se soočajo z operativnimi izzivi pri tem, kako sami na usklajen in stroškovno učinkovit način obravnavati tveganje na področju IKT in blažiti škodljive vplive incidentov na področju IKT.

(11) Ker enotnih pravil ni spremljal celovit okvir za tveganja na področju IKT ali operativna tveganja, je potrebna nadaljnja harmonizacija ključnih zahtev glede digitalne operativne odpornosti za vse finančne subjekte. Razvoj zmožnosti IKT in splošna odpornost finančnih subjektov na podlagi teh ključnih zahtev, da bi ti lahko prenesli prekinitve poslovanja, bi pomagali ohranjati stabilnost in celovitost finančnih trgov Unije in tako prispevali k zagotavljanju visoke ravni zaščite vlagateljev in potrošnikov v Uniji. Ker je namen te uredbe prispevati k nemotenemu delovanju notranjega trga, bi morala temeljiti na določbah člena 114 Pogodbe o delovanju Evropske unije (PDEU), kot se razlagajo v skladu z ustaljeno sodno prakso Sodišča Evropske unije (v nadaljnjem besedilu: Sodišče).

(12) Namen te uredbe je konsolidirati in nadgraditi zahteve glede tveganja na področju IKT kot del zahtev glede operativnega tveganja, ki so bile do zdaj obravnavane ločeno v različnih pravnih aktih Unije. Ti akti so zajemali glavne kategorije finančnega tveganja (npr. kreditno tveganje, tržno tveganje, kreditno tveganje nasprotne stranke in likvidnostno tveganje, tveganje ravnanja na trgu), vendar v času sprejetja niso celovito obravnavali vseh elementov operativne odpornosti. Pravila glede operativnih tveganj, ki so bila nadalje razvita v teh pravnih aktih Unije, so pogosto dajala prednost tradicionalnemu kvantitativnemu pristopu k obravnavanju tveganj (zlasti določitev kapitalske zahteve za pokritje tveganja na področju IKT) namesto ciljno usmerjenih kvalitativnih pravil glede zmožnosti za zaščito, odkrivanje, omejitev, okrevanje in popravila v zvezi z incidenti, povezanimi z IKT, ali glede

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

zmožnosti za poročanje in digitalno testiranje. Ti akti naj bi predvsem zajeli in posodobili bistvena pravila o bonitetnem nadzoru, celovitosti trga ali ravnanju na trgu. S konsolidacijo in nadgradnjo različnih pravil o tveganju na področju IKT bi se morale vse določbe, ki obravnavajo digitalno tveganje v finančnem sektorju, prvič dosledno združiti v enem samem zakonodajnem aktu. Zato ta uredba zapolnjuje vrzeli ali odpravlja nedoslednosti v nekaterih prejšnjih pravnih aktih, tudi v zvezi s terminologijo, ki se v njih uporablja, in se izrecno sklicuje na tveganje na področju IKT prek ciljno usmerjenih pravil o zmožnostih obvladovanja tveganj na področju IKT, poročanju o incidentih, testiranju operativne odpornosti in spremljanju tveganja tretjih strani na področju IKT. Ta uredba bi morala tako okrepiti tudi ozaveščenost o tveganju na področju IKT in potrditi, da incidenti na področju IKT in pomanjkanje operativne odpornosti lahko ogrozijo trdnost finančnih subjektov.

(13) Finančni subjekti bi morali pri obravnavanju tveganja na področju IKT uporabljati enak pristop in enaka pravila, ki temeljijo na načelih, pri tem pa bi bilo treba upoštevati njihovo velikost in splošni profil tveganja ter naravo, obseg in kompleksnost njihovih storitev, dejavnosti in poslovanja. Doslednost prispeva k povečanju zaupanja v finančni sistem in ohranjanju njegove stabilnosti, zlasti v časih velike odvisnosti od sistemov, platform in infrastruktur IKT, ki prinaša tudi povečano digitalno tveganje. Upoštevanje osnovne kibernetske higiene bi moralo preprečiti tudi nastajanje znatnih stroškov za gospodarstvo z zmanjšanjem učinkov in stroškov motenj na področju IKT na najmanjšo možno mero.

(14) Uredba na splošno pomaga zmanjšati regulativno kompleksnost, spodbuja konvergenco nadzora in povečuje pravno varnost ter prispeva k omejevanju stroškov izpolnjevanja obveznosti, zlasti za finančne subjekte, ki poslujejo na čezmejni podlagi, in k zmanjšanju izkrivljanja konkurence. Zato je izbira uredbe za vzpostavitev skupnega okvira za digitalno operativno odpornost finančnih subjektov najustreznejši način za zagotovitev homogene in skladne uporabe vseh elementov obvladovanja tveganj na področju IKT v finančnem sektorju Unije.

(15) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta ([7]) je bila prvi horizontalni okvir za kibernetsko varnost, uveljavljen na ravni Unije, in se je uporabljala tudi za tri vrste finančnih subjektov, in sicer za kreditne institucije, mesta trgovanja in centralne nasprotne stranke. Ker pa je bil v Direktivi (EU) 2016/1148 določen mehanizem določitve izvajalcev bistvenih storitev na nacionalni ravni, so bile v praksi le nekatere kreditne institucije, mesta trgovanja in centralne nasprotne stranke, ki so jih določile države članice, zajete v njeno področje uporabe in primorane izpolnjevati zahteve glede varnosti IKT in obveščanja o incidentih, določene v njej. Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta ([8]) določa enotno merilo za določitev subjektov, ki spadajo na njeno področje uporabe (pravilo o mejni vrednosti za velikost), hkrati pa na svojem področju uporabe ohranja tudi tri vrste finančnih subjektov.

(16) Ker pa ta uredba z uvedbo zahtev glede obvladovanja tveganja na področju IKT in poročanja o incidentih, povezanih z IKT, ki so strožje v primerjavi s tistimi, ki jih določa veljavno pravo Unije o finančnih storitvah, viša raven harmonizacije različnih elementov digitalne odpornosti, ta višja raven pomeni večjo harmonizacijo tudi v primerjavi z zahtevami iz Direktive (EU) 2022/2555. Posledično je ta uredba *lex specialis* glede na Direktivo (EU) 2022/2555. Hkrati je ključno, da se ohrani močna povezava med finančnim sektorjem in horizontalnim okvirom Unije za kibernetsko varnost, kot je trenutno določen v Direktivi (EU) 2022/2555, da bi se zagotovila skladnost s strategijami kibernetske varnosti, ki so jih sprejele države članice, in da bi se finančnim nadzornikom omogočilo, da se seznanijo s kibernetskimi incidenti, ki prizadenejo druge sektorje, zajete v navedeni direktivi.

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

([8]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (grej stran 80 tega Uradnega lista).

(17) V skladu s členom 4(2) Pogodbe o Evropski uniji in brez poseganja v sodni nadzor Sodišča ta uredba ne bi smela vplivati na odgovornost držav članic v zvezi s temeljnimi državnimi funkcijami, ki zadevajo javno varnost, obrambo in varovanje nacionalne varnosti, na primer kar zadeva zagotavljanje informacij, ki bi bile v nasprotju z varovanjem nacionalne varnosti.

(18) Da bi se omogočilo medsektorsko učenje in bi se učinkovito črpalo iz izkušenj drugih sektorjev pri obravnavanju kibernetskih groženj, bi morali finančni subjekti iz Direktive (EU) 2022/2555 ostati del „ekosistema“ navedene direktive (na primer Skupina za sodelovanje in skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT)). Evropski nadzorni organi in nacionalni pristojni organi bi morali imeti možnost sodelovati v razpravah o strateških politikah in pri tehničnem delu Skupine za sodelovanje na podlagi te direktive ter si izmenjevati informacije in nadalje sodelovati z enotnimi kontaktnimi točkami, imenovanimi ali vzpostavljenimi v skladu z navedeno direktivo. Pristojni organi na podlagi te uredbe bi se morali posvetovati tudi s skupinami CSIRT in z njimi sodelovati. Pristojni organi bi morali imeti tudi možnost, da za tehnični nasvet zaprosijo pristojne organe, imenovane ali ustanovljene v skladu z Direktivo (EU) 2022/2555, in vzpostavijo ureditve sodelovanja, katerih namen je zagotovitev učinkovitih in hitrih mehanizmov usklajevanja.

(19) Glede na močne medsebojne povezave med digitalno odpornostjo in fizično odpornostjo finančnih subjektov je v tej uredbi in Direktivi (EU) 2022/2557 Evropskega parlamenta in Sveta ([9]) potreben usklajen pristop do odpornosti kritičnih subjektov. Glede na to, da se fizična odpornost finančnih subjektov celostno obravnava z obveznostmi glede obvladovanja tveganj na področju IKT in poročanja o njem, ki jih zajema ta uredba, se obveznosti iz poglavij III in IV Direktive (EU)2022/2557 ne bi smele uporabljati za finančne subjekte, ki spadajo na področje uporabe navedene direktive.

(20) Ponudniki storitev računalništva v oblaku so ena od kategorij digitalne infrastrukture, ki jo zajema Direktiva (EU) 2022/2555. Okvir nadzora Unije (v nadaljnjem besedilu: okvir nadzora), vzpostavljen s to uredbo, se uporablja za vse ključne tretje ponudnike storitev IKT, vključno s ponudniki storitev računalništva v oblaku, ki opravljajo storitve IKT za finančne subjekte, in bi ga bilo treba obravnavati kot dopolnitev nadzora na podlagi Direktive (EU) 2022/2555. Poleg tega bi moral okvir nadzora, vzpostavljen s to uredbo, zajemati ponudnike storitev računalništva v oblaku, saj ni horizontalnega okvira Unije, ki bi vzpostavljal organ za digitalni nadzor.

(21) Da bi se ohranil polni nadzor nad tveganjem na področju IKT, bi morali imeti finančni subjekti celostne zmožnosti, ki bi omogočile trdno in učinkovito obvladovanje tveganj na področju IKT, ter specifične mehanizme in politike za obravnavanje vseh incidentov, povezanih z IKT, in za poročanje o večjih incidentih, povezanih z IKT. Podobno bi morali imeti finančni subjekti vzpostavljene politike za testiranje sistemov, kontrol in postopkov IKT ter za obvladovanje tveganja tretjih strani na področju IKT. Minimalne zahteve glede digitalne operativne odpornosti za finančne subjekte bi bilo treba povečati, hkrati pa tudi omogočiti, da se zahteve sorazmerno uporabljajo za določene finančne subjekte, zlasti mikropodjetja, kot tudi finančne subjekte, za katere se uporablja poenostavljen okvir za obvladovanje tveganj na področju IKT. Za olajšanje učinkovitega nadzora institucij za poklicno pokojninsko zavarovanje, ki je sorazmeren in upošteva potrebo po zmanjšanju upravnih bremen za pristojne organe, bi bilo treba pri ustreznih nacionalnih nadzornih ureditvah v zvezi s takimi finančnimi subjekti upoštevati njihovo velikost in celoten profil tveganja ter naravo, obseg in kompleksnost njihovih storitev, dejavnosti in poslovanja, tudi ko so zadevni pragovi, določeni v členu 5 Direktive (EU) 2016/2341 Evropskega parlamenta in Sveta ([10]) preseženi. Zlasti bi se morale nadzorne dejavnosti osredotočati predvsem na potrebo po obravnavanju resnih tveganj, povezanih z obvladovanjem tveganj na področju IKT, določenega subjekta.

([9]) Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (glej stran 164 tega Uradnega lista).

([10]) Direktiva (EU) 2016/2341 Evropskega parlamenta in Sveta z dne 14. decembra 2016 o dejavnostih in nadzoru institucij za poklicno pokojninsko zavarovanje (UL L 354, 23.12.2016, str. 37).

Pristojni organi bi morali imeti pozoren, vendar sorazmeren pristop v zvezi z nadzorom institucij za poklicno pokojninsko zavarovanje, ki v skladu s členom 31 Direktive (EU) 2016/2341 znaten del svojih osnovnih dejavnosti, kot so upravljanje sredstev, aktuarski izračuni, računovodstvo in upravljanje podatkov, oddajo v zunanje izvajanje ponudnikom storitev.

(22) Pragovi in taksonomije poročanja o incidentih, povezanih z IKT, se na nacionalni ravni zelo razlikujejo. Z ustreznim delom Agencije Evropske unije za kibernetsko varnost (ENISA), ustanovljene z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([11]), in Skupine za sodelovanje iz Direktive (EU) 2022/2555 je sicer mogoče doseči skupno podlago, vendar za preostale finančne subjekte še vedno obstajajo ali se lahko pojavijo različni pristopi glede določanja pragov in uporabe taksonomij. Zaradi te raznolikosti obstajajo številne zahteve, ki jih morajo izpolnjevati finančni subjekti, zlasti ko poslujejo v več državah članicah in kadar so del finančne skupine. Poleg tega bi lahko take razlike ovirale vzpostavitev nadaljnjih enotnih ali centraliziranih mehanizmov Unije, ki pospešujejo postopek poročanja in podpirajo hitro in nemoteno izmenjavo informacij med pristojnimi organi, kar je bistvenega pomena za obravnavo tveganja na področju IKT v primeru obsežnih napadov s potencialno sistemskimi posledicami.

(23) Za zmanjšanje upravnega bremena in potencialno podvojenih obveznosti poročanja za nekatere finančne subjekte bi se morale zahteve za poročanje o incidentih na podlagi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta ([12]) prenehati uporabljati za ponudnike plačilnih storitev, ki spadajo na področje uporabe te uredbe. Zato bi morali kreditne institucije, institucije za izdajo elektronskega denarja, plačilne institucije in ponudniki storitev zagotavljanja informacij o računih iz člena 33(1) navedene direktive od datuma začetka uporabe te uredbe naprej na podlagi te uredbe poročati o vseh operativnih incidentih ali varnostnih incidentih, povezanih s plačili, o katerih se je prej poročalo na podlagi navedene direktive, ne glede na to, ali so taki incidenti povezani z IKT.

(24) S to uredbo bi bilo treba določiti trdno ureditev poročanja o incidentih, povezanih z IKT, pri čemer bi zadevne zahteve zapolnile trenutne vrzeli v pravu na področju finančnih storitev, ter odpraviti obstoječa prekrivanja in podvajanja za znižanje stroškov, da bi lahko pristojni organi izpolnjevali nadzorno vlogo, tako da bi pridobili celovit vpogled v naravo, pogostost, pomen in učinek incidentov, povezanih z IKT, ter da bi se okrepila izmenjava informacij med ustreznimi javnimi organi, vključno z organi kazenskega pregona in organi za reševanje. Nujno je treba harmonizirati ureditev poročanja o incidentih, povezanih z IKT, tako da se od vseh finančnih subjektov zahteva, naj poročajo svojim pristojnim organom v okviru enotnega usklajenega okvira, kot je določen v tej uredbi. Poleg tega bi morali biti evropski nadzorni organi pooblaščeni za nadaljnjo opredelitev relevantnih elementov za okvir poročanja o incidentih, povezanih z IKT, kot so taksonomija, časovni okviri, nabori podatkov, predloge in veljavni pragovi. Da bi se zagotovila popolna usklajenost z Direktivo (EU) 2022/2555, bi moralo biti finančnim subjektom omogočeno, da pomembne kibernetske grožnje prostovoljno priglasijo ustreznemu pristojnemu organu, kadar menijo, da je kibernetska grožnja relevantna za finančni sistem, uporabnike storitev ali stranke.

(25) V nekaterih finančnih podsektorjih so se oblikovale zahteve glede testiranja digitalne operativne odpornosti, na podlagi katerih so nastali okviri, ki niso vedno v celoti usklajeni. To vodi v morebitno podvajanje stroškov za čezmejne finančne subjekte, vzajemno priznavanje rezultatov testiranja digitalne operativne odpornosti pa je bolj kompleksno, kar lahko vodi v fragmentacijo notranjega trga.

([11]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

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

(26) Poleg tega, kadar se testiranje IKT ne zahteva, ranljivosti ostanejo neodkrite in posledično so finančni subjekti izpostavljeni tveganju na področju IKT, kar nazadnje vodi do večjega tveganja za stabilnost in celovitost finančnega sektorja. Brez posredovanja Unije bi bilo testiranje digitalne operativne odpornosti še naprej nedosledno in ne bi bilo sistema vzajemnega priznavanja rezultatov testiranja IKT v različnih jurisdikcijah. Ker poleg tega ni verjetno, da bi drugi finančni podsektorji v večjem obsegu sprejeli ureditve testiranja, bi bili prikrajšani za potencialne koristi okvira testiranja v smislu razkritja ranljivosti in tveganj na področju IKT ter testiranja obrambnih zmožnosti in neprekinjenega poslovanja, ki prispeva k večanju zaupanja strank, dobaviteljev in poslovnih partnerjev. Za odpravo teh prekrivanj, razhajanj in vrzeli je treba določiti pravila za usklajeno ureditev testiranja in tako olajšati vzajemno priznavanje naprednega testiranja za finančne subjekte, ki izpolnjujejo merila, določena v tej uredbi.

(27) Odvisnost finančnih subjektov od uporabe storitev IKT deloma temelji na njihovi potrebi po tem, da se prilagodijo nastajajočemu konkurenčnemu digitalnemu svetovnemu gospodarstvu, povečajo svojo poslovno učinkovitost in zadostijo povpraševanju potrošnikov. Narava in obseg te odvisnosti sta se v zadnjih letih nenehno spreminjala, kar je povzročilo zniževanje stroškov v finančnem posredništvu ter omogočilo širjenje poslovanja in nadgradljivost pri uvajanju finančnih dejavnosti, hkrati pa zagotovilo široko paleto orodij IKT za upravljanje kompleksnih notranjih postopkov.

(28) Obsežna uporaba storitev IKT se kaže v kompleksnih pogodbenih dogovorih, pri čemer imajo finančni subjekti pogosto težave pri pogajanjih o pogodbenih pogojih, ki so prilagojeni bonitetnim standardom ali drugim regulativnim zahtevam, ki jih zavezujejo, ali sicer pri uveljavljanju posebnih pravic, kot so pravice do dostopa ali revizije, tudi če so slednje vključene v njihove pogodbene dogovore. Poleg tega veliko teh pogodbenih dogovorov ne zagotavlja zadostnih zaščitnih ukrepov, ki bi omogočali celovito spremljanje postopkov oddaje v podizvajanje, zaradi česar finančni subjekt ne more oceniti s tem povezanih tveganj. Ker poleg tega tretji ponudniki storitev IKT pogosto opravljajo standardizirane storitve za različne vrste strank, taki pogodbeni dogovori ne zadovoljijo vedno ustrezno posameznih ali posebnih potreb akterjev v finančnem sektorju.

(29) Čeprav pravo Unije na področju finančnih storitev vsebuje nekatera splošna pravila o zunanjem izvajanju, spremljanje pogodbenega vidika ni v celoti vključeno v pravo Unije. Ker ni jasnih in prilagojenih standardov Unije, ki bi veljali za pogodbene dogovore, sklenjene s tretjimi ponudniki storitev IKT, zunanji vir tveganja na področju IKT ni v celoti obravnavan. Zato je treba določiti nekatera ključna načela za usmerjanje finančnih subjektov pri obvladovanju tveganja tretjih strani na področju IKT, ki so zlasti pomembna, kadar se finančni subjekti za podporo svojih kritičnih ali pomembnih funkcij obrnejo na tretje ponudnike storitev IKT. Ta načela bi moral spremljati sklop temeljnih pogodbenih pravic v zvezi z več elementi pri izvajanju in prenehanju pogodbenih dogovorov, da se zagotovijo nekateri minimalni zaščitni ukrepi za okrepitev zmožnosti finančnih subjektov, da učinkovito spremljajo vsa tveganja na področju IKT, ki nastanejo na ravni tretjih ponudnikov storitev. Ta načela dopolnjujejo sektorsko pravo, ki se uporablja za zunanje izvajanje.

(30) Danes se kaže določeno pomanjkanje homogenosti in konvergence v zvezi s spremljanjem tveganja tretjih strani na področju IKT in odvisnosti od tretjih strani na področju IKT. Kljub prizadevanjem za obravnavo zunanjega izvajanja, kot so smernice EBA o zunanjem izvajanju iz leta 2019 in smernice ESMA o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku iz leta 2021, širše vprašanje boja proti sistemskemu tveganju, ki bi ga lahko povzročila izpostavljenost finančnega sektorja omejenemu številu ključnih tretjih ponudnikov storitev IKT, v pravu Unije ni zadostno obravnavano. Pomanjkanje pravil na ravni Unije dodatno stopnjuje neobstoj nacionalnih pravil o pooblastilih in orodjih, ki bi finančnim nadzornikom omogočala dobro razumevanje odvisnosti od tretjih strani na področju IKT in ustrezno spremljanje tveganj, ki izhajajo iz koncentracije odvisnosti od tretjih strani na področju IKT.

(31) Ob upoštevanju potencialnega sistemskega tveganja, ki ga prinašajo pogostejše prakse oddajanja v zunanje izvajanje in koncentracija tretjih strani na področju IKT, ter ob upoštevanju nezadostnosti nacionalnih mehanizmov, ki bi finančnim nadzornikom zagotovili zadostna orodja za količinsko in kakovostno opredelitev ter odpravo posledic tveganja na področju IKT, ki se pojavlja pri ključnih tretjih ponudnikih storitev IKT, je treba vzpostaviti ustrezen okvir nadzora, ki omogoča stalno spremljanje dejavnosti tretjih ponudnikov storitev IKT, ki so ključni tretji ponudniki storitev IKT za finančne subjekte, ob hkratnem zagotavljanju, da se ohranita zaupnost in varnost strank, ki niso finančni subjekti. Čeprav opravljanje storitev IKT znotraj skupine prinaša posebna tveganja in koristi, se ne bi smelo samodejno šteti za manj tvegano, kot je opravljanje storitev IKT s strani ponudnikov, ki niso del finančne skupine, in bi zato zanj moral veljati isti regulativni okvir. Vendar pa če se storitve IKT opravljajo v okviru iste finančne skupine, imajo lahko finančni subjekti višjo raven kontrole nad ponudniki znotraj skupine, kar bi bilo treba upoštevati pri splošni oceni tveganja.

(32) Ker tveganje na področju IKT postaja vse bolj kompleksno in izpopolnjeno, so dobri ukrepi za odkrivanje in preprečevanje tveganja na področju IKT v veliki meri odvisni od redne izmenjave obveščevalnih podatkov o grožnjah in ranljivostih med finančnimi subjekti. Izmenjava informacij prispeva k boljši ozaveščenosti o kibernetskih grožnjah. To nasprotno povečuje zmogljivost finančnih subjektov, da preprečijo, da bi kibernetske grožnje postale dejanski incidenti, povezani z IKT, ter finančnim subjektom omogoča, da uspešneje zajezijo vpliv incidentov, povezanih z IKT, ter hitreje okrevajo. Videti je, da ob pomanjkanju smernic na ravni Unije več dejavnikov ovira tako izmenjavo obveščevalnih podatkov, zlasti negotovost glede združljivosti s pravili o varstvu podatkov, protimonopolnimi pravili in pravili o odgovornosti.

(33) Poleg tega se koristne informacije zadržujejo zaradi dvomov glede vrste informacij, ki se lahko delijo z drugimi udeleženci na trgu ali z nenadzornimi organi (kot sta ENISA za analitični prispevek ali Europol za namene kazenskega pregona). Zato obseg in kakovost izmenjave informacij zato trenutno ostajata omejena in razdrobljena, pri čemer ustrezne izmenjave večinoma potekajo na lokalni ravni (prek nacionalnih pobud) in brez skladnih dogovorov o izmenjavi informacij na ravni Unije, ki bi bili prilagojeni potrebam celostnega finančnega sistema. Zato je pomembno okrepiti te komunikacijske kanale.

(34) Finančne subjekte bi bilo treba spodbuditi, da si medsebojno izmenjujejo informacije in obveščevalne podatke o kibernetskih grožnjah ter skupaj izkoristijo individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmožnosti za ustrezno ocenjevanje in spremljanje kibernetskih groženj, obrambo pred njimi in odzivanje nanje, in sicer tako, da sodelujejo pri dogovorih o izmenjavi informacij. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij, ki bi, kadar bi se izvajali v zaupanja vrednih okoljih, skupnosti finančnega sektorja pomagali, da preprečuje kibernetske grožnje in se skupaj odziva nanje s hitrim omejevanjem širjenja tveganja na področju IKT in preprečevanjem morebitnega širjenja negativnih učinkov po finančnih kanalih. Ti mehanizmi bi morali biti skladni z veljavnimi pravili konkurenčnega prava Unije, določenimi v sporočilu Komisije z dne 14. januarja 2011 z naslovom "Smernice o uporabi člena 101 Pogodbe o delovanju Evropske unije za sporazume o horizontalnem sodelovanju" in pravili Unije o varstvu podatkov, zlasti Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ([13]). Delovati bi morali na podlagi uporabe ene ali več pravnih podlag iz člena 6 navedene uredbe, na primer v okviru obdelave osebnih podatkov, ki je potrebna za namene pravnega interesa upravljavca ali tretje strani, kot je navedeno v členu 6(1), točka (f), navedene uredbe, ter v okviru obdelave osebnih podatkov, ki je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca, in je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, kot je navedeno v členu 6(1), točka (c) oziroma (e), navedene uredbe.

([13]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

(35) Da bi se ohranila visoka raven digitalne operativne odpornosti za celoten finančni sektor in bi se hkrati sledilo tehnološkemu razvoju, bi morala ta uredba obravnavati tveganje, ki izhaja iz vseh vrst storitev IKT. V ta namen bi bilo treba opredelitev storitev IKT v okviru te uredbe razumeti široko, tako da zajema digitalne in podatkovne storitve, ki se prek sistemov IKT stalno opravljajo za enega ali več notranjih ali zunanjih uporabnikov. Ta opredelitev bi morala na primer vključevati tako imenovane povrhnje storitve, ki spadajo v kategorijo elektronskih komunikacijskih storitev. Izključiti bi morala le omejeno kategorijo tradicionalnih analognih telefonskih storitev, ki se štejejo za storitve javnega komutiranega telefonskega omrežja (PSTN), storitve stacionarnega omrežja, tradicionalne telefonske storitve (POTS) ali fiksne telefonske storitve.

(36) Ne glede na široko pokritost, predvideno s to uredbo, bi bilo treba pri uporabi pravil o digitalni operativni odpornosti upoštevati pomembne razlike med finančnimi subjekti glede njihove velikosti in splošnega profila tveganja. Načeloma bi morali finančni subjekti pri dodeljevanju virov in zmožnosti za izvajanje okvira za obvladovanje tveganj na področju IKT najti ustrezno ravnotežje med svojimi potrebami v zvezi z IKT ter svojo velikostjo in splošnim profilom tveganja ter naravo, obsegom in kompleksnostjo svojih storitev, dejavnosti in poslovanja, pristojni organi pa bi morali še naprej ocenjevati in pregledovati pristop takega dodeljevanja.

(37) Ponudniki storitev zagotavljanja informacij o računih iz člena 33(1) Direktive (EU) 2015/2366 so izrecno vključeni v področje uporabe te uredbe, pri čemer se upoštevajo posebna narava njihovih dejavnosti in tveganja, ki izhajajo iz njih. Poleg tega so institucije za izdajo elektronskega denarja in plačilne institucije, ki so izvzete na podlagi člena 9(1) Direktive 2009/110/ES Evropskega parlamenta in Sveta ([14]) ter člena 32(1) Direktive (EU) 2015/2366, vključene na področje uporabe te uredbe, tudi če jim v skladu z Direktivo 2009/110/ES ni bilo izdano dovoljenje za izdajanje elektronskega denarja ali če jim v skladu z Direktivo (EU) 2015/2366 ni bilo izdano dovoljenje za opravljanje in izvrševanje plačilnih storitev. Vendar so poštne institucije, ki opravljajo storitev brezgotovinskega nakazovanja, iz člena 2(5), točka 3, Direktive 2013/36/EU Evropskega parlamenta in Sveta ([15]) izključene s področja uporabe te uredbe. Pristojni organ za plačilne institucije, izvzete na podlagi Direktive (EU) 2015/2366, institucije za izdajo elektronskega denarja, izvzete na podlagi Direktive 2009/110/ES, in ponudnike storitev zagotavljanja informacij o računih iz člena 33(1) Direktive (EU) 2015/2366 bi moral biti pristojni organ, imenovan v skladu s členom 22 Direktive (EU) 2015/2366.

(38) Ker imajo večji finančni subjekti lahko na razpolago precejšnje vire in lahko hitro namenijo sredstva za razvoj struktur upravljanja in oblikovanje različnih poslovnih strategij, bi se moralo le od finančnih subjektov, ki niso mikropodjetja v smislu te uredbe, zahtevati, naj vzpostavijo kompleksnejše ureditve upravljanja. Taki subjekti so zlasti bolje opremljeni, da vzpostavijo namenske funkcije upravljanja za nadziranje dogovorov s tretjimi ponudniki storitev IKT ali obvladovanje kriz, svoje obvladovanje tveganj na področju IKT organizirajo v skladu z modelom treh obrambnih linij ali vzpostavijo notranji model obvladovanja in nadzorovanja tveganj ter svoj okvir za obvladovanje tveganj na področju IKT predložijo v notranjo revizijo.

(39) Za nekatere finančne subjekte veljajo izjeme ali zelo ohlapen regulativni okvir na podlagi ustreznega sektorskega prava Unije. Taki finančni subjekti vključujejo upravitelje alternativnih investicijskih skladov iz člena 3(2) Direktive 2011/61/EU Evropskega parlamenta in Sveta ([16]), zavarovalnice in pozavarovalnice iz člena 4 Direktive 2009/138/ES Evropskega parlamenta in Sveta ([17]) ter institucije za poklicno pokojninsko zavarovanje, ki upravljajo pokojninske načrte, ki skupaj nimajo več kot 15 članov. Glede na te izjeme vključitev takih finančnih subjektov na

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

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

([16]) Direktiva 2011/61/EU Evropskega parlamenta in Sveta z dne 8. junija 2011 o upraviteljih alternativnih investicijskih skladov in spremembah direktiv 2003/41/ES in 2009/65/ES ter uredb (ES) št. 1060/2009 in (EU) št. 1095/2010 (UL L 174, 1.7.2011, str. 1).

([17]) Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).

področje uporabe te uredbe ne bi bila sorazmerna. Poleg tega ta uredba priznava posebnosti strukture trga zavarovalnega posredništva, zato se ne bi smela uporabljati za zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj, ki se uvrščajo med mikropodjetja ali med mala ali srednja podjetja.

(40) Ker so subjekti iz člena 2(5), točke 4 do 23, Direktive 2013/36/EU izključeni s področja uporabe navedene direktive, bi morale države članice posledično imeti možnost, da iz uporabe te uredbe izvzamejo te subjekte, ki se nahajajo na njihovem ozemlju.

(41) Podobno je za uskladitev te uredbe s področjem uporabe Direktive 2014/65/EU Evropskega parlamenta in Sveta ([18]) ustrezno, da se s področja uporabe te uredbe izključijo tudi fizične in pravne osebe iz členov 2 in 3 navedene direktive, ki lahko opravljajo investicijske storitve, ne da bi jim bilo treba pridobiti dovoljenje na podlagi Direktive 2014/65/EU. Vendar člen 2 Direktive 2014/65/EU s področja uporabe navedene direktive izključuje tudi subjekte, ki se za namene te uredbe štejejo za finančne subjekte, kot so centralne depotne družbe, kolektivni naložbeni podjemi ali zavarovalnice in pozavarovalnice. Izključitev oseb in subjektov iz členov 2 in 3 navedene direktive s področja uporabe te uredbe ne bi smelo zajemati teh centralnih depotnih družb, kolektivnih naložbenih podjemov ali zavarovalnic in pozavarovalnic.

(42) V skladu s sektorskim pravom Unije za nekatere finančne subjekte veljajo manj stroge zahteve ali izvzetja iz razlogov, povezanih z njihovo velikostjo ali storitvami, ki jih opravljajo. Ta kategorija finančnih subjektov vključuje mala in nepovezana investicijska podjetja, male institucije za poklicno pokojninsko zavarovanje, ki jih zadevna država članica lahko izključi s področja uporabe Direktive (EU) 2016/2341 pod pogoji iz člena 5 navedene direktive in upravljajo pokojninske načrte, ki skupaj nimajo več kot 100 članov, ter institucije, izvzete na podlagi Direktive 2013/36/EU. Zato je v skladu z načelom sorazmernosti in za ohranitev duha sektorskega prava Unije ustrezno, da se tudi za navedene finančne subjekte uporablja poenostavljen okvir za obvladovanje tveganj na področju IKT na podlagi te uredbo. Regulativni tehnični standardi, ki naj bi jih razvili evropski nadzorni organi, ne bi smeli spreminjati sorazmerne narave okvira za obvladovanje tveganj na področju IKT, ki zajema te finančne subjekte. Poleg tega je v skladu z načelom sorazmernosti ustrezno, da se tudi za plačilne institucije iz člena 32(1) Direktive (EU) 2015/2366 in institucije za izdajo elektronskega denarja iz člena 9 Direktive 2009/110/ES, ki so izvzete v skladu z nacionalnim pravom za prenos teh pravnih aktov Unije, uporablja poenostavljen okvir za obvladovanje tveganj na področju IKT na podlagi te uredbe, medtem ko bi morale plačilne institucije in institucije za izdajo elektronskega denarja, ki v skladu z zadevnim nacionalnim pravom za prenos sektorskega prava Unije niso bile izvzete, izpolnjevati zahteve splošnega okvira iz te uredbe.

(43) Podobno se od finančnih subjektov, ki so mikropodjetja ali za katere se uporablja poenostavljen okvir za obvladovanje tveganj na področju IKT na podlagi te uredbe, ne bi smelo zahtevati, da določijo vlogo za spremljanje dogovorov, sklenjenih s tretjimi ponudniki storitev IKT o uporabi storitev IKT, ali določijo člana višjega vodstva, ki bo odgovoren za nadzor s tem povezane izpostavljenosti tveganju in ustrezne dokumentacije, da odgovornost za obvladovanje tveganj na področju IKT in nadzor nad njimi dodelijo nadzorni funkciji in zagotovijo, da ima taka nadzorna funkcija ustrezno raven neodvisnosti, da bi se preprečila nasprotja interesov, da dokumentirajo in pregledajo najmanj enkrat letno okvir za obvladovanje tveganj na področju IKT, da redno izvajajo notranjo revizijo okvira za obvladovanje tveganj na področju IKT, da izvedejo poglobljene ocene po večjih spremembah v svojem omrežju ter infrastrukturi in procesih informacijskega sistema, da redno izvajajo analize tveganj za obstoječe sisteme IKT, da opravljajo neodvisne notranje revizije izvajanja načrtov odzivanja in okrevanja IKT, da imajo funkcijo obvladovanja kriz, da razširijo testiranje načrtov za neprekinjeno poslovanje ter odzivanje in okrevanje, da bi zajeli scenarije preklopa med primarno infrastrukturo IKT in redundantnimi sistemi, da pristojnim organom na njihovo zahtevo poročajo o oceni skupnih letnih stroškov in izgub, ki nastanejo zaradi večjih incidentov, povezanih z IKT, da ohranjajo redundantne zmogljivosti IKT, da nacionalnim pristojnim organom sporočijo spremembe,

([18]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).

izvedene na podlagi opravljenih pregledov po incidentih, povezanih z IKT, da stalno spremljajo ustrezen tehnološki razvoj, da vzpostavijo celosten program testiranja digitalne operativne odpornosti kot sestavni del okvira za obvladovanje tveganj na področju IKT iz te uredbe ali da sprejmejo in redno pregledujejo strategijo o tveganju tretjih strani na področju IKT. Od mikropodjetij bi bilo treba dodatno zahtevati le, da ocenijo potrebo po ohranjanju takih redundantnih zmogljivosti IKT na podlagi svojega profila tveganja. Mikropodjetja bi morala imeti koristi od prožnejše ureditve v zvezi s programi testiranja digitalne operativne odpornosti. Pri razmisleku o vrsti in pogostosti testiranja, ki ga je treba opraviti, bi morala ustrezno uravnotežiti cilj ohranjanja visoke digitalne operativne odpornosti, razpoložljive vire in svoj splošni profil tveganja. Mikropodjetja in finančne subjekte, za katere se uporablja poenostavljeni okvir za obvladovanje tveganj na področju IKT na podlagi te uredbe, bi bilo treba izvzeti iz zahteve po opravljanju naprednega testiranja orodij, sistemov in postopkov IKT, ki temelji na penetracijskem testiranju na podlagi analize groženj, saj bi bilo treba izvedbo takega testiranja zahtevati le od finančnih subjektov, ki izpolnjujejo merila, določena v tej uredbi. Glede na svoje omejene zmožnosti bi morala imeti mikropodjetja možnost, da se s tretjim ponudnikom storitev IKT dogovorijo o prenosu pravic finančnega subjekta glede dostopa, inšpekcijskega pregleda in revizije na neodvisno tretjo stran, ki jo imenuje tretji ponudnik storitev IKT, pod pogojem, da lahko finančni subjekt od zadevne neodvisne tretje strani kadar koli zahteva vse zadevne informacije in zagotovilo o uspešnosti tretjega ponudnika storitev IKT.

(44) Ker bi morali penetracijsko testiranje na podlagi analize groženj izvajati le tisti finančni subjekti, ki so bili določeni za namene naprednega testiranja digitalne odpornosti, bi moral upravne postopke in finančne stroške, povezane z izvajanjem takih testov, nositi le majhen delež finančnih subjektov.

(45) Upravljalni organi finančnih subjektov bi morali ohraniti ključno in aktivno vlogo pri usmerjanju in prilagajanju okvira za obvladovanje tveganj na področju IKT in splošne strategije za digitalno operativno odpornost, da se zagotovi popolna uskladitev in splošna skladnost med poslovnimi strategijami finančnih subjektov na eni strani in obvladovanjem tveganja na področju IKT na drugi strani. Pristop upravljalnih organov se ne bi smel osredotočati le na sredstva za zagotavljanje odpornosti sistemov IKT, temveč bi moral vključevati tudi ljudi in postopke, in sicer s sklopom politik, ki na vsaki ravni podjetja in pri vseh zaposlenih vzbujajo močan občutek zavedanja o kibernetskih tveganjih in zavezanost spoštovanju stroge kibernetske higiene na vseh ravneh. Končna odgovornost upravljalnega organa pri upravljanju tveganj finančnega subjekta na področju IKT bi morala biti poglavitno načelo tega celostnega pristopa, ki se nadalje prenese v stalno sodelovanje upravljalnega organa pri nadzoru nad spremljanjem obvladovanja tveganj na področju IKT.

(46) Poleg tega je načelo polne in končne odgovornosti upravljalnega organa za obvladovanje tveganj finančnega subjekta na področju IKT tesno povezano s potrebo po zagotovitvi določene ravni naložb, povezanih z IKT, in splošnega proračuna za finančni subjekt, ki bi finančnemu subjektu omogočil, da doseže visoko raven digitalne operativne odpornosti.

(47) Ta uredba črpa navdih iz ustreznih mednarodnih, nacionalnih in panožnih najboljših praks, smernic, priporočil in pristopov k obvladovanju kibernetskih tveganj in spodbuja vrsto načel, ki lajšajo splošno strukturiranje obvladovanja tveganj na področju IKT. Posledično dokler se z najpomembnejšimi zmožnostmi, ki jih vzpostavijo finančni subjekti, obravnavajo različne funkcije pri obvladovanju tveganj na področju IKT (prepoznavanje, zaščita in preprečevanje, odkrivanje, odzivanje in okrevanje, učenje in razvoj ter komunikacija), določene v tej uredbi, bi morali finančni subjekti imeti možnost, da uporabljajo modele obvladovanja tveganj na področju IKT, ki so oblikovani ali kategorizirani drugače.

(48) Da bi se sledilo spreminjajočemu se okolju kibernetskih groženj, bi morali finančni subjekti vzdrževati posodobljene sisteme IKT, ki so zanesljivi in zmožni ne le zagotavljati obdelavo podatkov, ki je potrebna za njihove storitve, temveč zagotavljati tudi zadostno tehnološko odpornost, ki jim omogoča, da se ustrezno spopadajo z dodatnimi potrebami po obdelavi podatkov, ki so posledica zaostrenih tržnih ali drugih neugodnih razmer.

(49) Potrebni so učinkoviti načrti neprekinjenega poslovanja in okrevanja, da lahko finančni subjekti takoj in hitro rešujejo incidente, povezane z IKT, zlasti kibernetske napade, tako da omejijo škodo in prednostno ponovno vzpostavijo dejavnosti in izvedejo ukrepe za okrevanje v skladu s svojimi politikami varnostnega kopiranja. Vendar takšna ponovna vzpostavitev nikakor ne bi smela ogroziti celovitosti in varnosti omrežnih in informacijskih sistemov oziroma razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti podatkov.

(50) Ta uredba finančnim subjektom omogoča, da prilagodljivo določijo svoje cilje glede časa za okrevanje in točke obnovitve in posledično take cilje določijo ob popolnem upoštevanju narave in kritičnosti zadevnih funkcij ter morebitnih posebnih poslovnih potreb, vendar bi se morala pri določanju takih ciljev zahtevati tudi ocena morebitnega splošnega vpliva na učinkovitost trga.

(51) Storilci kibernetskih napadov si običajno prizadevajo za finančne koristi neposredno pri viru, zato so finančni subjekti izpostavljeni znatnim posledicam. Da sistemi IKT ne bi izgubili celovitosti ali postali nerazpoložljivi ter da bi se tako izognili kršitvam v zvezi s podatki in poškodovanju fizične infrastrukture IKT, bi bilo treba znatno izboljšati in racionalizirati poročanje finančnih subjektov o večjih incidentih, povezanih z IKT. Poročanje o večjih incidentih, povezanih z IKT, bi bilo treba harmonizirati z uvedbo zahteve, da morajo vsi finančni subjekti poročati neposredno svojim ustreznim pristojnim organom. Kadar finančni subjekt nadzira več kot en nacionalni pristojni organ, bi morale države članice kot naslovnika takšnega poročanja določiti en sam pristojni organ. Kreditne institucije, razvrščene kot pomembne v skladu s členom 6(4) Uredbe Sveta (EU) št. 1024/2013 ([19]), bi morale takšno poročanje predložiti nacionalnim pristojnim organom, ki bi morali nato poročilo posredovati Evropski centralni banki (ECB).

(52) Neposredno poročanje bi moralo finančnim nadzornikom omogočiti takojšen dostop do informacij o večjih incidentih, povezanih z IKT. Finančni nadzorniki bi nasprotno morali podrobnosti o večjih incidentih, povezanih z IKT, posredovati javnim nefinančnim organom (kot so pristojni organi in enotne kontaktne točke na podlagi Direktive (EU) 2022/2555, nacionalni organi za varstvo podatkov in organi kazenskega pregona za večje incidente, povezane z IKT, ki so kazenske narave), da bi se izboljšala ozaveščenost teh organov o takih incidentih, ter v primeru skupin CSIRT, da bi se olajšalo hitro zagotavljanje pomoči, ki se lahko da na voljo finančnim subjektom, kot je ustrezno. Države članice bi poleg tega morale imeti možnost določiti, da bi morali finančni subjekti sami zagotavljati take informacije javnim organom zunaj področja finančnih storitev. Ti tokovi informacij bi morali finančnim subjektom omogočiti, da hitro izkoristijo vse ustrezne tehnične prispevke, nasvete o popravnih ukrepih in nadaljnje ukrepe teh organov. Informacije o večjih incidentih, povezanih z IKT, bi morale teči obojestransko: finančni nadzorniki bi morali finančnemu subjektu zagotoviti vse potrebne povratne informacije ali smernice, evropski nadzorni organi pa bi morali deliti anonimizirane podatke o kibernetskih grožnjah in ranljivostih v zvezi z incidentom, da bi pripomogli k širši kolektivni obrambi.

(53) Medtem ko bi morali biti vsi finančni subjekti dolžni poročati o incidentih, ta zahteva verjetno ne bo zadevala vseh na enak način. Ustrezne pragove pomembnosti ter roke za poročanje bi bilo treba ustrezno prilagoditi v kontekstu delegiranega akta na podlagi regulativnih tehničnih standardov, ki jih razvijejo evropski nadzorni organi, da bi zajeli le večje incidente, povezane z IKT. Poleg tega bi bilo treba pri določanju rokov za obveznosti poročanja upoštevati posebnosti finančnih subjektov.

(54) Ta uredba bi morala od kreditnih institucij, plačilnih institucij, ponudnikov storitev zagotavljanja informacij o računih in institucij za izdajo elektronskega denarja zahtevati, da poročajo o vseh operativnih incidentih ali varnostnih incidentih, povezanih s plačili, o katerih se je predhodno poročalo na podlagi Direktive (EU) 2015/2366, ne glede na to, ali je incident IKT narave ali ne.

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

(55) Evropskim nadzornim organom bi bilo treba naložiti, naj ocenijo izvedljivost in pogoje za morebitno centralizacijo poročil o incidentih, povezanih z IKT, na ravni Unije. Taka centralizacija bi lahko pomenila enotno vozlišče EU za poročanje o večjih incidentih, povezanih z IKT, ki bi bodisi neposredno prejemalo zadevna poročila in samodejno obveščalo nacionalne pristojne organe ali zgolj centraliziralo zadevna poročila, ki jih posredujejo nacionalni pristojni organi, in tako imelo koordinacijsko vlogo. Evropskim nadzornim organom bi bilo treba naložiti, da v posvetovanju z ECB in ENISA pripravijo skupno poročilo, v katerem preučijo izvedljivost vzpostavitve enotnega vozlišča EU.

(56) Da bi se dosegla visoka raven digitalne operativne odpornosti, ki je skladna tako z relevantnimi mednarodnimi standardi (kot so temeljni elementi za penetracijsko testiranje na podlagi analize groženj skupine G7) kot z okviri, ki se uporabljajo v Uniji, kot je okvir TIBER–EU, bi morali finančni subjekti svoje sisteme IKT in zaposlene, ki imajo odgovornosti, povezane z IKT, redno testirati glede učinkovitosti njihovih zmožnosti preprečevanja, odkrivanja, odzivanja in okrevanja, da bi se odkrile in odpravile morebitne ranljivosti na področju IKT. Da bi se odražale obstoječe razlike med različnimi finančnimi podsektorji in znotraj njih glede ravni pripravljenosti finančnih subjektov na področju kibernetske varnosti, bi moralo testiranje vključevati širok nabor orodij in ukrepov, od ocene osnovnih zahtev (npr. ocene in pregledi ranljivosti, analize prosto dostopnih virov, ocene varnosti omrežja, analize vrzeli, pregledi fizične varnosti, vprašalniki in rešitve programske opreme za pregledovanje, pregledi izvorne kode, kadar je to mogoče, testiranja na podlagi scenarijev, testiranje združljivosti, testiranje učinkovitosti ali celovito testiranje) do naprednejšega testiranja s penetracijskim testiranjem na podlagi analize groženj. Tako naprednejše testiranje bi bilo treba zahtevati le za finančne subjekte, ki so z vidika IKT dovolj pripravljeni, da ga lahko razumno izvedejo. Testiranje digitalne operativne odpornosti, ki se zahteva s to uredbo, bi zato moralo biti za tiste finančne subjekte, ki izpolnjujejo merila, določena v tej uredbi, (na primer velike, sistemske kreditne institucije, ki dosegajo zrelost na področju IKT, borze vrednostnih papirjev, centralne depotne družbe in centralne nasprotne stranke) zahtevnejše kot za druge finančne subjekte. Hkrati bi moralo biti testiranje digitalne operativne odpornosti s penetracijskim testiranjem na podlagi analize groženj pomembnejše za finančne subjekte, ki delujejo v osrednjih podsektorjih finančnih storitev in imajo sistemsko vlogo (na primer plačila, bančništvo ter kliring in poravnava), in manj pomembno za druge podsektorje (na primer upravljavci premoženja in bonitetne agencije).

(57) Finančni subjekti, ki sodelujejo v čezmejnih dejavnostih in uveljavljajo svobodo do ustanavljanja ali do opravljanja storitev v Uniji, bi morali v svoji matični državi članici izpolnjevati enoten sklop zahtev za napredno testiranje (kot je penetracijsko testiranje na podlagi analize groženj), ki bi moralo vključevati infrastrukture IKT v vseh jurisdikcijah, kjer čezmejna finančna skupina posluje znotraj Unije, kar bi takim čezmejnim finančnim skupinam omogočilo, da stroške testiranja, povezanega z IKT, nosijo le v eni jurisdikciji.

(58) Da bi se črpalo iz strokovnega znanja, ki so ga nekateri pristojni organi že pridobili, zlasti v zvezi z izvajanjem okvira TIBER-EU, bi morala ta uredba državam članicam omogočiti, da na nacionalni ravni imenujejo en sam javni organ, ki je v finančnem sektorju odgovoren za vsa vprašanja z zvezi s penetracijskim testiranjem na podlagi analize groženj, ali – če tak organ ni imenovan – da pristojni organi izvajanje nalog, povezanih s penetracijskim testiranjem na podlagi analize groženj, prenesejo na drug nacionalni finančni pristojni organ.

(59) Ker ta uredba od finančnih subjektov ne zahteva, da z enim samim penetracijskim testiranjem na podlagi analize groženj pokrijejo vse kritične ali pomembne funkcije, bi morali finančni subjekti imeti možnost, da sami določijo, katere in koliko kritičnih ali pomembnih funkcij bi bilo treba vključiti v okvir takega testiranja.

(60) Skupno testiranje v smislu te uredbe – kadar v penetracijskem testiranju na podlagi analize groženj sodeluje več finančnih subjektov in kadar lahko tretji ponudnik storitev IKT sklene pogodbene dogovore neposredno z zunanjim preizkuševalcem, – bi lahko bilo dovoljeno le, kadar je mogoče razumno pričakovati, da to ne bo škodljivo vplivalo na kakovost ali varnost storitev, ki jih tretji ponudnik storitev IKT zagotavlja strankam, ki so subjekti zunaj področja uporabe te uredbe, ali zaupnost podatkov v zvezi s temi storitvami. Za skupno testiranje bi morali veljati tudi zaščitni ukrepi (usmerjanje s strani enega imenovanega finančnega subjekta, prilagoditev števila sodelujočih finančnih subjektov), da bi se za sodelujoče finančne subjekte zagotovilo strogo testiranje, ki izpolnjuje cilje penetracijskega testiranja na podlagi analize groženj na podlagi te uredbe.

(61) Da bi se izkoristili notranji viri, ki so na voljo na ravni podjetja, bi morala ta uredba omogočiti, da bi penetracijsko testiranje na podlagi analize groženj izvajali notranji preizkuševalci, pod pogojem, da je bila izdana nadzorna odobritev, da ni nasprotij interesov, in da se redno (po vsakih treh testih) menjajo notranji in zunanji preizkuševalci, hkrati pa subjekt, ki v okviru penetracijskega testiranja na podlagi analize groženj zagotavlja obveščevalne podatke o grožnjah, nikoli ne sme biti del finančnega subjekta. Za izvajanje penetracijskega testiranja na podlagi analize groženj bi moral biti v celoti odgovoren finančni subjekt. Potrdila, ki jih predložijo organi, bi morala biti namenjena izključno vzajemnemu priznavanju in ne bi smela izključevati nadaljnjih ukrepov, potrebnih za obravnavanje tveganja na področju IKT, ki mu je izpostavljen finančni subjekt, niti se ne bi smela šteti kot nadzorna odobritev zmožnosti finančnega subjekta za obvladovanje in zmanjševanje tveganj na področju IKT.

(62) Da bi se zagotovilo učinkovito spremljanje tveganja tretjih strani na področju IKT v finančnem sektorju, je treba določiti sklop na načelih temelječih pravil, ki bodo finančnim subjektom zagotavljala usmeritve pri spremljanju tveganja, ki izhaja iz oddajanja funkcij v zunanje izvajanje tretjim ponudnikom storitev IKT, zlasti za storitve IKT, ki podpirajo kritične ali pomembne funkcije, in splošneje, iz vseh odvisnosti od tretjih strani na področju IKT.

(63) Da bi se obravnavala kompleksnost različnih virov tveganja na področju IKT ob hkratnem upoštevanju številnih in raznolikih ponudnikov tehnoloških rešitev, ki omogočajo nemoteno opravljanje finančnih storitev, bi morala ta uredba pokrivati širok sklop tretjih ponudnikov storitev IKT, vključno s ponudniki storitev računalništva v oblaku, programske opreme in storitev analize podatkov ter ponudniki storitev podatkovnih centrov. Ker bi morali finančni subjekti učinkovito in usklajeno identificirati in obvladovati vse vrste tveganja, tudi v okviru storitev IKT, ki se pridobijo znotraj finančne skupine, je treba pojasniti, da bi bilo treba kot tretje ponudnike storitev IKT na podlagi te uredbe šteti tudi podjetja, ki so del finančne skupine in opravljajo storitve IKT predvsem za svoje obvladujoče podjetje ali odvisna podjetja ali podružnice svojega obvladujočega podjetja, kot tudi finančne subjekte, ki opravljajo storitve IKT za druge finančne subjekte. Nazadnje, bi bilo treba glede na razvoj trga plačilnih storitev, ki postaja vse bolj odvisen od kompleksnih tehničnih rešitev, in glede na nove vrste plačilnih storitev in s plačili povezanih rešitev kot tretje ponudnike storitev IKT na podlagi te uredbe šteti tudi udeležence v ekosistemu plačilnih storitev, ki opravljajo dejavnosti obdelave plačil ali upravljajo plačilne infrastrukture, z izjemo centralnih bank, kadar upravljajo plačilne sisteme ali sisteme poravnave vrednostnih papirjev, in javnih organov, kadar storitve, povezane z IKT, opravljajo v okviru izpolnjevanja državnih funkcij.

(64) Finančni subjekt bi moral biti ves čas v celoti odgovoren za izpolnjevanje svojih obveznosti iz te uredbe. Finančni subjekti bi morali slediti sorazmernemu pristopu k spremljanju tveganj, ki se pojavljajo na ravni tretjih ponudnikov storitev IKT, tako da ustrezno preučijo naravo, obseg, kompleksnost in pomen svojih odvisnosti, povezanih z IKT, kritičnost ali pomen storitev, postopkov ali funkcij, za katere veljajo pogodbeni dogovori, in nazadnje natančno ocenijo morebitni vpliv na kontinuiteto in kakovost finančnih storitev na ravni posameznika in skupine, kot je ustrezno.

(65) Tako spremljanje bi se moralo izvajati na podlagi strateškega pristopa k tveganju tretjih strani na področju IKT, ki je bil formaliziran s sprejetjem posebne strategije glede tveganja tretjih strani na področju IKT s strani upravljalnega organa finančnega subjekta, in temeljiti na nenehnem preverjanju vseh odvisnosti od tretjih strani na področju IKT. Da bi se povečala ozaveščenost nadzornikov o odvisnosti od tretjih strani na področju IKT in bi se dodatno podprlo delo v kontekstu okvira nadzora, vzpostavljenega s to uredbo, bi bilo treba od vseh finančnih subjektov zahtevati, da vodijo register informacij z vsemi pogodbenimi dogovori o uporabi storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT. Finančni nadzorniki bi morali imeti možnost, da zahtevajo dostop do celotnega registra ali njegovih posameznih delov in tako pridobijo bistvene informacije za dosego širšega razumevanja odvisnosti finančnih subjektov na področju IKT.

(66) Temeljita analiza, opravljena vnaprej pred sklenitvijo pogodbe, bi morala biti podlaga za formalno sklenitev pogodbenih dogovorov, zlasti z osredotočanjem na elemente, kot so kritičnost ali pomembnost storitev, podprtih s predvideno pogodbo o IKT, potrebne nadzorne odobritve ali drugi pogoji, morebitno tveganje koncentracije, uporaba potrebne skrbnosti v postopku izbire in ocenjevanja tretjih ponudnikov storitev IKT ter ocenjevanje morebitnih nasprotij interesov. Pri pogodbenih dogovorih, ki zadevajo kritične ali pomembne funkcije, bi morali finančni subjekti upoštevati, ali tretji ponudniki storitev IKT uporabljajo najnovejše in najvišje standarde informacijske varnosti. Na prenehanje pogodbenih dogovorov bi lahko vplivala vsaj vrsta okoliščin, ki kažejo na pomanjkljivosti na ravni tretjega ponudnika storitev IKT, zlasti pomembne kršitve prava ali pogodbenih pogojev, okoliščine, ki kažejo na morebitne spremembe pri opravljanju funkcij, opredeljenih v pogodbenih dogovorih,

dokazila o šibkih točkah tretjega ponudnika storitev IKT v celotnem okviru obvladovanja tveganj na področju IKT, ali okoliščine, ki kažejo na nezmožnost ustreznih pristojnih organov, da učinkovito nadzirajo finančni subjekt.

(67) Za obravnavo sistemskega vpliva tveganja koncentracije tretjih strani na področju IKT ta uredba spodbuja uravnoteženo rešitev, in sicer sprejetje prilagodljivega in postopnega pristopa k takšnemu koncentriranemu tveganju, saj bi lahko naložitev katere koli neprilagodljive zgornje meje ali strogih omejitev ovirala poslovanje in omejevala pogodbeno svobodo. Finančni subjekti bi morali temeljito oceniti svoje predvidene pogodbene dogovore, da bi prepoznali verjetnost pojava takega tveganja, tudi s poglobljenimi analizami dogovorov o podizvajanju, zlasti kadar so sklenjeni s tretjimi ponudniki storitev IKT s sedežem v tretji državi. V tej fazi in zaradi doseganja poštenega ravnovesja med nujnostjo ohranjanja pogodbene svobode in nujnostjo zagotavljanja finančne stabilnosti se ne zdi ustrezno, da bi se določila pravila za stroge zgornje meje in omejitve v zvezi z izpostavljenostjo tretjim stranem na področju IKT. V kontekstu okvira nadzora bi moral glavni nadzornik, imenovan na podlagi te uredbe, v zvezi s ključnimi tretjimi ponudniki storitev IKT posebno pozornost nameniti temu, da bi v celoti razumel razsežnost soodvisnosti, odkril posebne primere, v katerih bo visoka stopnja koncentracije ključnih tretjih ponudnikov storitev IKT v Uniji verjetno obremenila stabilnost in celovitost finančnega sistema Unije, ter ob prepoznavi takega specifičnega tveganja ohranjal dialog s ključnimi tretjimi ponudniki storitev IKT.

(68) Za redno ocenjevanje in spremljanje zmožnosti tretjega ponudnika storitev IKT, da finančnemu subjektu varno opravlja storitve brez škodljivih učinkov na digitalno operativno odpornost finančnega subjekta, bi bilo treba harmonizirati več ključnih pogodbenih elementov s tretjimi ponudniki storitev IKT. Taka harmonizacija bi morala zajemati najmanj področja, ki so ključna za to, da lahko finančni subjekt celostno spremlja tveganja, ki bi lahko izhajala od tretjega ponudnika storitev IKT, in sicer z vidika potrebe finančnega subjekta, da zaščiti svojo digitalno odpornost, saj je v veliki meri odvisna od stabilnosti, funkcionalnosti, razpoložljivosti in varnosti prejetih storitev IKT.

(69) Pri ponovnih pogajanjih o pogodbenih dogovorih za uskladitev z zahtevami te uredbe bi morali finančni subjekti in tretji ponudniki storitev IKT zagotoviti, da so zajete ključne pogodbene določbe iz te uredbe.

(70) Opredelitev „kritične ali pomembne funkcije“ iz te uredbe zajema opredelitev „kritičnih funkcij“ iz člena 2(1), točka (35), Direktive 2014/59/EU Evropskega parlamenta in Sveta ([20]). Tako so funkcije, ki veljajo za kritične na podlagi Direktive 2014/59/EU, vključene v opredelitev kritičnih funkcij v smislu te uredbe.

(71) Ne glede na kritičnost ali pomembnost funkcije, ki jo podpirajo storitve IKT, bi morali pogodbeni dogovori zlasti vsebovati specifikacijo podrobnih opisov funkcij in storitev, lokacij, na katerih se zagotavljajo take funkcije in kjer se bodo obdelovali podatki, ter navedbo opisov ravni storitev. Drugi bistveni elementi, ki finančnemu subjektu omogočajo spremljanje tveganja tretjih strani na področju IKT so: pogodbene določbe, ki določajo, kako tretji ponudnik storitev IKT zagotavlja dostopnost, razpoložljivost, celovitost, varnost in varstvo osebnih podatkov, določbe za ustrezna jamstva, ki omogočajo dostopnost, reševanje in vračilo podatkov v primeru insolventnosti, reševanja ali prenehanja poslovanja tretjega ponudnika storitev IKT, ter določbe, ki od tretjega ponudnika storitev IKT zahtevajo, da zagotovi pomoč v primeru incidentov IKT, povezanih s storitvami, ki jih opravlja, in sicer brez dodatnih stroškov ali z vnaprej določenimi stroški; določbe o obveznosti tretjega ponudnika storitev IKT, da v celoti sodeluje s pristojnimi organi in organi za reševanje finančnega subjekta, ter določbe o pravicah do odpovedi in

([20]) Direktiva 2014/59/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o vzpostavitvi okvira za sanacijo ter reševanje kreditnih institucij in investicijskih podjetij ter o spremembi Šeste direktive Sveta 82/891/EGS ter direktiv 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU in 2013/36/EU in uredb (EU) št. 1093/2010 ter (EU) št. 648/2012 Evropskega parlamenta in Sveta (UL L 173, 12.6.2014, str. 190).

povezanih minimalnih rokih za odpoved pogodbenih dogovorov v skladu s pričakovanji pristojnih organov in organov za reševanje.

(72) Poleg takih pogodbenih določb in da se zagotovi, da finančni subjekti ohranijo popoln nadzor nad vsemi dogodki na ravni tretjih oseb, ki bi lahko škodovali njihovi varnosti IKT, bi morale pogodbe za zagotavljanje storitev IKT, ki podpirajo kritične ali pomembne funkcije, določati tudi naslednje: specifikacijo vseh opisov ravni storitev z natančnimi kvantitativnimi in kvalitativnimi cilji uspešnosti, da se brez nepotrebnega odlašanja omogočijo ustrezni korektivni ukrepi, kadar dogovorjene ravni storitev niso dosežene; ustrezne odpovedne roke in obveznosti poročanja tretjega ponudnika storitev IKT v primeru sprememb, ki bi lahko pomembno vplivale na zmožnost tretjega ponudnika storitev IKT, da učinkovito opravlja svoje zadevne storitve IKT; zahtevo, da tretji ponudnik storitev IKT izvaja in testira poslovne načrte izrednih ukrepov ter vzpostavi varnostne ukrepe, orodja in politike na področju IKT, ki omogočajo varno opravljanje storitev, ter da je vključen v penetracijsko testiranje na podlagi analize groženj, ki ga izvaja finančni subjekt, in pri tem v celoti sodeluje.

(73) Pogodbe za opravljanje storitev IKT, ki podpirajo kritične ali pomembne funkcije, bi morale vsebovati tudi določbe, ki omogočajo pravice do dostopa, inšpekcijskega pregleda in revizije s strani finančnega subjekta ali imenovane tretje strani, in pravico do izdelave kopij kot ključnega instrumenta v okviru stalnega spremljanja uspešnosti tretjega ponudnika storitev IKT, ki ga izvaja finančni subjekt, pri čemer ponudnik storitev med inšpekcijskimi pregledi polno sodeluje. Podobno bi moral imeti pristojni organ finančnega subjekta na podlagi obvestil pravico, da pri tretjem ponudniku storitev IKT opravi inšpekcijski pregled in revizijo, pri čemer mora varovati zaupne informacije.

(74) Taki pogodbeni dogovori bi morali določati tudi namenske izhodne strategije, ki bi omogočile zlasti obvezna prehodna obdobja, v katerih bi morali tretji ponudniki storitev IKT še naprej opravljati ustrezne storitve, da bi se zmanjšalo tveganje motenj na ravni finančnega subjekta ali bi se slednjemu omogočilo, da začne učinkovito uporabljati storitve drugih tretjih ponudnikov storitev IKT ali da preide na notranje rešitve, ki ustrezajo kompleksnosti opravljene storitve IKT. Poleg tega bi morali finančni subjekti, ki spadajo na področje uporabe Direktive 2014/59/EU, zagotoviti, da so zadevne pogodbe za storitve IKT trdne in v celoti izvršljive, če se ti finančni subjekti znajdejo v postopku reševanja. Zato bi morali ti finančni subjekti v skladu s pričakovanji organov za reševanje zagotoviti, da na zadevne pogodbe za storitve IKT reševanje ne vpliva. Dokler ti finančni subjekti še naprej izpolnjujejo svoje plačilne obveznosti, bi morali med drugim zagotoviti, da zadevne pogodbe za storitve IKT vsebujejo klavzule, da teh pogodb zaradi prestrukturiranja ali reševanja ni mogoče odpovedati, začasno prekiniti in spremeniti.

(75) Poleg tega bi lahko prostovoljna uporaba standardnih pogodbenih klavzul, ki jih je razvil javni organ ali institucija Unije, zlasti uporaba pogodbenih klavzul, ki jih je razvila Komisija za storitve računalništva v oblaku, finančnim subjektom in tretjim ponudnikom storitev IKT dala dodatno zagotovilo, saj bi se zvišala stopnja njihove pravne varnosti glede uporabe storitev računalništva v oblaku v finančnem sektorju, in sicer v polni skladnosti z zahtevami in pričakovanji iz prava Unije o finančnih storitvah. Razvoj standardnih pogodbenih klavzul temelji na ukrepih, predvidenih že v akcijskem načrtu za finančno tehnologijo iz leta 2018, v katerem je Komisija objavila svojo namero, da spodbudi in olajša oblikovanje standardnih pogodbenih klavzul, na podlagi katerih finančni subjekti oddajo storitve računalništva v oblaku v zunanje izvajanje, pri čemer se opira na medsektorska prizadevanja deležnikov na področju storitev računalništva v oblaku, ki jih je Komisija podprla skupaj s sodelovanjem finančnega sektorja.

(76) Za ključne tretje ponudnike storitev IKT bi moral veljati okvir nadzora Unije, da bi se spodbudili konvergenca in učinkovitost pristopov nadzora v zvezi z obravnavanjem tveganja tretjih strani na področju IKT v finančnem sektorju ter okrepila digitalna operativna odpornost finančnih subjektov, ki so za opravljanje storitve IKT, ki podpirajo zagotavljanje finančnih storitev, odvisni od ključnih tretjih ponudnikov storitev IKT, s čimer bi se prispevalo k ohranjanju stabilnosti finančnega sistema Unije in celovitosti notranjega trga finančnih storitev. Čeprav

je vzpostavitev okvira nadzora upravičena zaradi dodane vrednosti ukrepanja na ravni Unije ter zaradi inherentne vloge in posebnosti uporabe storitev IKT pri opravljanju finančnih storitev, bi bilo treba hkrati opozoriti, da se ta rešitev zdi primerna le v okviru te uredbe, ki posebej obravnava digitalno operativno odpornost v finančnem sektorju. Vendar takšen okvir nadzora ne bi smel veljati kot nov model za nadzor Unije na drugih področjih finančnih storitev in dejavnosti.

(77) Okvir nadzora bi se moral uporabljati samo za ključne tretje ponudnike storitev IKT. Zato bi moral obstajati mehanizem imenovanja, ki bi upošteval razsežnost in naravo odvisnosti finančnega sektorja od takih tretjih ponudnikov storitev IKT. Ta mehanizem bi moral vključevati sklop kvantitativnih in kvalitativnih meril za določitev parametrov kritičnosti kot podlage za vključitev v okvir nadzora. Za zagotovitev točnosti te ocene in ne glede na podjetniško strukturo tretjega ponudnika storitev IKT bi morala taka merila v primeru tretjega ponudnika storitev IKT, ki je del širše skupine, upoštevati celotno strukturo skupine tretjega ponudnika storitev IKT. Po drugi strani bi morali ključni tretji ponudniki storitev IKT, ki niso samodejno imenovani na podlagi uporabe navedenih meril, imeti možnost, da se prostovoljno vključijo v okvir nadzora, na drugi strani pa bi bilo treba izvzeti tretje ponudnike storitev IKT, za katere že veljajo okviri mehanizmov nadzora, ki podpirajo izpolnjevanje nalog Evropskega sistema centralnih bank iz člena 127(2) PDEU.

(78) Podobno bi morali biti tudi finančni subjekti, ki opravljajo storitve IKT za druge finančne subjekte, čeprav spadajo v kategorijo tretjih ponudnikov storitev IKT na podlagi te uredbe, izvzeti iz okvira nadzora, saj zanje že veljajo mehanizmi nadzora, vzpostavljeni z ustreznim pravom Unije o finančnih storitvah. Kadar je ustrezno, bi morali pristojni organi v okviru svojih nadzornih dejavnosti upoštevati tveganje na področju IKT, ki ga za finančne subjekte predstavljajo finančni subjekti, ki opravljajo storitve IKT. Prav tako bi bilo treba zaradi obstoječih mehanizmov za spremljanje tveganja na ravni skupine uvesti enako izjemo za tretje ponudnike storitev IKT, ki opravljajo storitve IKT predvsem za subjekte znotraj svoje skupine. Iz mehanizma imenovanja bi morali biti izvzeti tudi tretji ponudniki storitev IKT, ki storitve IKT opravljajo samo v eni državi članici za finančne subjekte, ki so dejavni samo v tej državi članici, saj je njihova dejavnost omejena in nima čezmejnega učinka.

(79) Z digitalno preobrazbo na področju finančnih storitev sta se kot še nikoli doslej povišali stopnja uporabe storitev IKT in odvisnost od njih. Ker si ni možno več predstavljati, da bi se finančne storitve opravljale brez uporabe storitev računalništva v oblaku, rešitev na področju programske opreme in podatkovnih storitev, je finančni ekosistem Unije postal neločljivo povezan z nekaterimi storitvami IKT, ki jih opravljajo ponudniki storitev IKT. Nekateri od teh ponudnikov, inovatorji pri razvoju in uporabi tehnologij, ki temeljijo na IKT, imajo pomembno vlogo pri zagotavljanju finančnih storitev ali so vključeni v vrednostno verigo finančnih storitev. Tako so postali ključni za stabilnost in integriteto finančnega sistema Unije. Ta vsesplošna odvisnost od storitev, ki jih zagotavljajo ključni tretji ponudniki storitev IKT, skupaj s soodvisnostjo informacijskih sistemov različnih upravljavcev trga ustvarja neposredno in potencialno resno tveganje za sistem finančnih storitev Unije in za neprekinjeno zagotavljanje finančnih storitev, če bi na ključne tretje ponudnike storitev IKT vplivale operativne motnje ali večji kibernetski incidenti. Kibernetski incidenti imajo posebno sposobnost, da se v celotnem finančnem sistemu razmnožujejo in širijo precej hitreje kot druge vrste tveganj, ki se spremljajo v finančnem sektorju, ter se lahko razširijo med sektorji in prek geografskih meja. Lahko se razvijejo v sistemsko krizo, pri čemer se zaupanje v finančni sistem zmanjša zaradi motnje v funkcijah, ki podpirajo realno gospodarstvo, ali znatnih finančnih izgub na ravni, ki je finančni sistem ne more prenesti ali ki zahteva uvedbo strogih ukrepov za absorbiranje pretresov. Da bi se preprečila uresničitev teh scenarijev in ogrožanje finančne stabilnosti in integritete Unije, je bistveno zagotoviti konvergenco nadzornih praks v zvezi s tveganji tretjih strani na področju IKT v finančnem sektorju, zlasti z novimi pravili, ki bi omogočala nadzor Unije nad ključnimi tretjimi ponudniki storitev IKT.

(80) Okvir nadzora je v veliki meri odvisen od stopnje sodelovanja med glavnim nadzornikom in ključnim tretjim ponudnikom storitev IKT, ki finančnim subjektom zagotavlja storitve, ki vplivajo na zagotavljanje finančnih storitev. Uspešen nadzor je med drugim odvisen od sposobnosti glavnega nadzornika, da učinkovito izvaja naloge spremljanja in inšpekcijske preglede za oceno pravil, kontrol in postopkov, ki jih uporabljajo ključni tretji ponudniki storitev IKT, ter za oceno morebitnega kumulativnega učinka njihovih dejavnosti na finančno stabilnost in integriteto finančnega sistema. Hkrati je zelo pomembno, da ključni tretji ponudniki storitev IKT upoštevajo priporočila glavnega nadzornika in obravnavajo njegove pomisleke. Če ključni tretji ponudnik storitev IKT, ki opravlja storitve, ki vplivajo na zagotavljanje finančnih storitev, ne bi sodeloval, tako da bi na primer zavrnil dostop do svojih prostorov ali ne bi predložil informacij, bi lahko glavni nadzornik ostal brez bistvenega orodja za ocenjevanje tveganja tretjih strani na področju IKT, kar bi lahko škodljivo vplivalo na finančno stabilnost in integriteto finančnega sistema, zato je treba zagotoviti tudi ustrezen režim sankcij.

(81) Glede na navedeno potreba glavnega nadzornika, da naloži denarne kazni, s katerimi ključne tretje ponudnike storitev IKT prisili k izpolnjevanju obveznosti v zvezi s preglednostjo in dostopom iz te uredbe, ne bi smela biti ogrožena zaradi težav pri izvrševanju teh denarnih kazni v zvezi s ključnimi tretjimi ponudniki storitev IKT s sedežem v tretjih državah. Da se zagotovi izvršljivost takih kazni in omogoči hitra uvedba postopkov za uveljavljanje pravic ključnih tretjih ponudnikov storitev IKT do obrambe v okviru mehanizma imenovanja in izdajanja priporočil, bi bilo treba od teh ključnih tretjih ponudnikov storitev IKT, ki za finančne subjekte opravljajo storitve, ki vplivajo na zagotavljanje finančnih storitev, zahtevati, da vzdržujejo ustrezno poslovno prisotnost v Uniji. Zaradi narave nadzora in ker v drugih jurisdikcijah ni primerljivih ureditev, ni ustreznih alternativnih mehanizmov, ki bi zagotovili ta cilj z učinkovitim sodelovanjem s finančnimi nadzorniki v tretjih državah v zvezi s spremljanjem učinka digitalnih operativnih tveganj, ki jih predstavljajo sistemski tretji ponudniki storitev IKT, ki se štejejo za ključne tretje ponudnike storitev IKT s sedežem v tretjih državah. Zato bi moral tretji ponudnik storitev IKT s sedežem v tretji državi, ki je bil v skladu s to uredbo imenovan za ključnega, da bi lahko še naprej opravljal svoje storitve za finančne subjekte Unije, v 12 mesecih od zadevnega imenovanja urediti vse potrebno za ureditev registracije v Uniji, tako da ustanovi odvisno podjetje, kot je opredeljeno v pravnem redu Unije, zlasti v Direktivi 2013/34/EU Evropskega parlamenta in Sveta ([21]).

(82) Zahteva po ustanovitvi odvisnega podjetja v Uniji ključnemu tretjemu ponudniku storitev IKT ne bi smela preprečevati zagotavljanja storitev IKT in povezane tehnične podpore iz objektov in infrastrukture, ki se nahajajo zunaj Unije. Ta uredba ne bi smela nalagati obveznosti lokalizacije podatkov, saj ne zahteva, da se podatki shranjujejo ali obdelujejo v Uniji.

(83) Ključni tretji ponudniki storitev IKT bi morali imeti možnost, da storitve IKT opravljajo kjer koli na svetu, ne nujno oziroma ne samo iz prostorov, ki se nahajajo v Uniji. Nadzorne dejavnosti bi bilo treba najprej izvajati v prostorih, ki se nahajajo v Uniji, in v sodelovanju s subjekti, ki se nahajajo v Uniji, vključno z odvisnimi podjetij, ki jih na podlagi te uredbe ustanovijo ključni tretji ponudniki storitev IKT. Vendar taki ukrepi v Uniji morda ne bodo zadostovali, da bi lahko glavni nadzornik v celoti in učinkovito opravljal svoje naloge na podlagi te uredbe. Glavni nadzornik bi zato moral imeti tudi možnost, da svoja ustrezna nadzorna pooblastila izvaja v tretjih državah. Izvajanje teh pooblastil v tretjih državah bi moralo glavnemu nadzorniku omogočiti, da pregleda objekte, iz katerih ključni tretji ponudnik storitev IKT dejansko opravlja ali upravlja storitve IKT ali storitve tehnične podpore, poleg tega pa bi mu moralo omogočiti tudi celovito in operativno razumevanje obvladovanja tveganj na področju IKT, ki ga izvaja ključni tretji ponudnik storitev IKT. Možnost glavnega nadzornika, da kot agencija Unije izvaja pooblastila zunaj ozemlja Unije, bi morala biti ustrezno urejena z ustreznimi pogoji, zlasti s privolitvijo zadevnega ključnega tretjega ponudnika storitev IKT. Podobno bi morali biti ustrezni organi tretje države obveščeni o izvajanju dejavnosti glavnega nadzornika na svojem ozemlju in mu ne nasprotujejo. Vendar pa morajo biti za zagotovitev učinkovitega izvajanja in brez poseganja v ustrezne pristojnosti institucij Unije in držav članic ta pooblastila v celoti vključena tudi v sklepanje dogovorov o upravnem sodelovanju z ustreznimi organi zadevne tretje države. Ta uredba bi zato morala evropskim nadzornim organom omogočiti, da sklenejo dogovore o upravnem sodelovanju

([21]) Direktiva 2013/34/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o letnih računovodskih izkazih, konsolidiranih računovodskih izkazih in povezanih poročilih nekaterih vrst podjetij, spremembi Direktive 2006/43/ES Evropskega parlamenta in Sveta ter razveljavitvi direktiv Sveta 78/660/EGS in 83/349/EGS (UL L 182, 29.6.2013, str. 19).

z ustreznimi organi tretjih držav, ki sicer ne bi smeli ustvarjati pravnih obveznosti za Unijo in njene države članice.

(84) Za lažjo komunikacijo z glavnim nadzornikom in zagotovitev ustrezne zastopanosti bi morali ključni tretji ponudniki storitev IKT, ki so del skupine, imenovati eno pravno osebo za svojo koordinacijsko točko.

(85) Okvir nadzora ne bi smel posegati v pristojnost držav članic za izvajanje lastnih nadzornih nalog ali nalog spremljanja v zvezi s tretjimi ponudniki storitev IKT, ki v skladu s to uredbo niso imenovani kot ključni, vendar se štejejo za pomembne na nacionalni ravni.

(86) Da bi se izkoristila večplastna institucionalna arhitektura na področju finančnih storitev, bi moral Skupni odbor evropskih nadzornih organov še naprej zagotavljati splošno medsektorsko usklajevanje v zvezi z vsemi zadevami, povezanimi s tveganji na področju IKT, v skladu s svojimi nalogami na področju kibernetske varnosti. Podpirati bi ga moral nov pododbor (v nadaljnjem besedilu: nadzorniški forum), ki bi izvajal pripravljalno delo tako za posamezne odločitve, naslovljene na ključne tretje ponudnike storitev IKT, kot za izdajanje skupnih priporočil, zlasti glede primerjalne analize programov nadzora nad ključnimi tretjimi ponudniki storitev IKT, ter opredeljeval najboljše prakse za obravnavo tveganj koncentracije na področju IKT.

(87) Za zagotovitev, da se ključne tretje ponudnike storitev IKT ustrezno in učinkovito nadzoruje na ravni Unije, ta uredba določa, da je lahko kateri koli od treh evropskih nadzornih organov imenovan za glavnega nadzornika. Dodelitev posameznega ključnega tretjega ponudnika storitev IKT enemu od treh evropskih nadzornih organov bi morala temeljiti na oceni prevladujoče narave finančnih subjektov, ki delujejo v finančnih sektorjih, za katere je odgovoren zadevni evropski nadzorni organ. S takim pristopom bi se morala doseči uravnotežena razdelitev nalog in odgovornosti med tremi evropskimi nadzornimi organi v okviru izvajanja nadzornih funkcij ter bi se morali čim bolje izkoristiti človeški viri in tehnično strokovno znanje, ki so na voljo v vsakem od treh evropskih nadzornih organov.

(88) Glavnim nadzornikom bi bilo treba dodeliti potrebna pooblastila za izvajanje preiskav, opravljanje inšpekcijskih pregledov na kraju samem in zunaj njega ključnih tretjih ponudnikov storitev IKT ter za pridobitev popolnih in posodobljenih informacij. Ta pooblastila bi morala glavnemu nadzorniku omogočiti, da pridobi pravi vpogled v vrsto, razsežnost in učinek tveganja tretjih strani na področju IKT za finančne subjekte in, nazadnje, za finančni sistem Unije. Podelitev glavne nadzorne vloge evropskim nadzornim organom je predpogoj za razumevanje in obravnavanje sistemske razsežnosti tveganj na področju IKT v finančnem sektorju. Zaradi vpliva ključnih tretjih ponudnikov storitev IKT na sektor finančnih storitev Unije in morebitnih težav, ki jih povzroča s tem povezano tveganje koncentracije na področju IKT, je potreben skupen pristop na ravni Unije. Sočasno ločeno izvajanje številnih revizij in pravic do dostopa s strani več pristojnih organov, pri katerem bi bilo usklajevanje omejeno ali pa ga sploh ne bi bilo, bi finančnim nadzornikom preprečilo pridobitev popolnega in celovitega pregleda nad tveganjem tretjih strani na področju IKT v Uniji, hkrati pa bi ustvarilo tudi odvečnost, breme in zapletenost za ključne tretje ponudnike storitev IKT, če bi se soočali s številnimi zahtevami za spremljanje in inšpekcijske preglede.

(89) Zaradi znatnega vpliva imenovanja za ključnega ponudnika bi bilo treba s to uredbo zagotoviti, da se pravice ključnih tretjih ponudnikov storitev IKT upoštevajo v celotnem izvajanju okvira nadzora. Preden se taki ponudniki imenujejo za ključne, bi morali taki ponudniki, na primer, imeti pravico, da glavnemu nadzorniku predložijo utemeljeno izjavo, ki bi vsebovala vse ustrezne informacije za namene ocene v zvezi z njihovim imenovanjem. Ker bi morali imeti glavni nadzorniki pooblastilo, da predložijo priporočila v zvezi s tveganji na področju IKT in ustreznimi popravnimi ukrepi, vključno s pooblastilom za nasprotovanje nekaterim pogodbenim dogovorom, ki nazadnje vplivajo na stabilnost finančnega subjekta ali finančnega sistema, bi morali imeti ključni tretji ponudniki

storitev IKT tudi možnost, da pred dokončnim oblikovanjem teh priporočil predložijo pojasnila o pričakovanem učinku rešitev, predvidenih v priporočilih, na stranke, ki so subjekti, ki ne spadajo na področje uporabe te uredbe, in oblikujejo rešitve za zmanjšanje tveganj. Ključni tretji ponudniki storitev IKT, ki se ne strinjajo s priporočili, bi morali predložiti utemeljeno obrazložitev svoje namere, da priporočila ne bodo potrdili. Kadar se taka utemeljena obrazložitev ne predloži ali kadar se šteje za nezadostno, bi moral glavni nadzornik izdati javno obvestilo s kratkim opisom vprašanja neskladnosti.

(90) Pristojni organi bi morali ustrezno vključiti nalogo preverjanja vsebinskega upoštevanja priporočil, ki jih izda glavni nadzornik, med svoje funkcije v zvezi z bonitetnim nadzorom finančnih subjektov. Pristojni organi bi morali imeti možnost, da od finančnih subjektov zahtevajo, da sprejmejo dodatne ukrepe za obravnavanje tveganj, opredeljenih v priporočilih glavnega nadzornika, in bi morali v ta namen pravočasno izdati obvestila. Kadar glavni nadzornik naslovi priporočila na ključne tretje ponudnike storitev IKT, ki so nadzorovani na podlagi Direktive (EU) 2022/2555, bi morali imeti pristojni organi možnost, da se pred sprejetjem dodatnih ukrepov prostovoljno posvetujejo s pristojnimi organi na podlagi navedene direktive, da bi spodbudili usklajen pristop pri obravnavi zadevnih ključnih tretjih ponudnikov storitev IKT.

(91) Izvajanje nadzora bi moralo temeljiti na treh operativnih načelih, ki naj bi zagotovila: (a) tesno usklajevanje med evropskimi nadzornimi organi v njihovi vlogi glavnih nadzornikov prek skupne nadzorne mreže, (b) skladnost z okvirom, vzpostavljenim z Direktivo (EU) 2022/2555 (s prostovoljnim posvetovanjem z organi na podlagi navedene direktive, da se prepreči podvajanje ukrepov, namenjenih ključnim tretjim ponudnikom storitev IKT), in (c) uporabo skrbnih pregledov za zmanjšanje morebitnega tveganja motenj storitev, ki jih ključni tretji ponudniki storitev IKT opravljajo za stranke, ki so subjekti, ki ne spadajo na področje uporabe te uredbe.

(92) Okvir nadzora ne bi smel zamenjati ali na kakršen koli način oziroma v kakšnem koli delu nadomestiti zahteve, da finančni subjekti sami obvladujejo tveganja, ki nastanejo v zvezi z uporabo tretjih ponudnikov storitev IKT, vključno z obveznostjo ohranjanja stalnega spremljanja pogodbenih dogovorov, sklenjenih s ključnimi tretjimi ponudniki storitev IKT. Prav tako okvir nadzora ne bi smel vplivati na polno odgovornost finančnih subjektov, da upoštevajo in izpolnijo vse pravne obveznosti iz te uredbe in ustreznega prava o finančnih storitvah.

(93) V izogib podvajanju in prekrivanju, pristojni organi ne bi smeli ločeno sprejemati ukrepov, namenjenih spremljanju tveganj ključnih tretjih ponudnikov storitev IKT, in bi se morali v zvezi s tem opirati na zadevno oceno glavnega nadzornika. Vsak ukrep bi bilo treba v vsakem primeru vnaprej uskladiti in se o njem dogovoriti **z** glavnim nadzornikom v okviru izvajanja nalog iz okvira nadzora.

(94) Evropske nadzorne organe bi bilo treba spodbujati, da sklenejo dogovore o sodelovanju z ustreznimi nadzornimi in regulativnimi organi tretjih držav, da bi se na mednarodni ravni spodbujala konvergenca glede uporabe najboljših praks pri reviziji in spremljanju obvladovanja digitalnih tveganj tretjih ponudnikov storitev IKT.

(95) Da bi se izkoristili posebne sposobnosti, tehnične spretnosti in strokovno znanje osebja, ki je specializirano za operativna tveganja in tveganja na področju IKT znotraj pristojnih organov, treh evropskih nadzornih organov in, na prostovoljni podlagi, pristojnih organov na podlagi Direktive (EU) 2022/2555, bi moral glavni nadzornik črpati iz nacionalnih nadzornih zmožnosti in znanja in za vsakega posameznega ključnega tretjega ponudnika storitev IKT ustanoviti posebne pregledniške ekipe, ki bi združevale multidisciplinarne skupine za podporo pri pripravi in izvajanju nadzornih dejavnosti, vključno s splošnimi preiskavami in inšpekcijskimi pregledi ključnih tretjih ponudnikov storitev IKT, ter pri vsakem potrebnem nadaljnjem spremljanju.

(96) Medtem ko bi se stroški, ki izhajajo iz nadzornih nalog, v celoti financirali z nadomestili, ki se zaračunavajo ključnim tretjim ponudnikom storitev IKT, bodo evropski nadzorni organi pred začetkom nadzornega okvira verjetno imeli stroške v zvezi z izvedbo namenskih sistemov IKT za podporo prihodnjemu nadzoru, saj bi bilo treba namenske sisteme IKT razviti in uvesti prej. Ta uredba zato določa model hibridnega financiranja, pri katerem bi se okvir nadzora kot tak v celoti financiral z nadomestili, medtem ko bi se razvoj sistemov IKT evropskih nadzornih organov financiral iz prispevkov Unije in pristojnih nacionalnih organov.

(97) Pristojni organi bi morali imeti vsa potrebna pooblastila za nadzor, preiskovanje in izrekanje sankcij, da se zagotovi pravilno izvrševanje njihovih nalog na podlagi te uredbe. Načeloma bi morali objaviti obvestila o upravnih kaznih, ki jih naložijo. Ker lahko imajo finančni subjekti in tretji ponudniki storitev IKT sedež v različnih državah članicah in so pod nadzorom različnih pristojnih organov, bi bilo treba uporabo te uredbe olajšati na eni strani s tesnim sodelovanjem med zadevnimi pristojnimi organi, vključno z ECB v zvezi s posebnimi nalogami, ki so nanjo prenesene z Uredbo Sveta (EU) št. 1024/2013, in na drugi strani s posvetovanjem z evropskimi nadzornimi organi prek vzajemne izmenjave informacij ter zagotavljanja pomoči pri ustreznih nadzornih dejavnostih.

(98) Za nadaljnjo kakovostno in količinsko opredelitev meril za imenovanje tretjih ponudnikov storitev IKT za ključne in za harmonizacijo nadomestil za nadzor bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte za dopolnitev te uredbe z nadaljnjo opredelitvijo sistemskega vpliva, ki bi ga prenehanje delovanja ali prekinitev poslovanja tretjega ponudnika storitev IKT lahko imelo na finančne subjekte, za katere opravlja storitve IKT, števila globalnih sistemsko pomembnih institucij ali drugih sistemsko pomembnih institucij, ki so odvisne od zadevnega tretjega ponudnika storitev IKT, števila tretjih ponudnikov storitev IKT, ki delujejo na določenem trgu, stroškov selitve podatkov in delovnih obremenitev IKT na druge tretje ponudnike storitev IKT ter zneska nadomestil za nadzor in načina njihovega plačila. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje ([22]). Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

(99) Regulativni tehnični standardi bi morali zagotoviti dosledno harmonizacijo zahtev iz te uredbe. Evropski nadzorni organi bi morali v vlogi organov z visoko specializiranim strokovnim znanjem pripraviti osnutke regulativnih tehničnih standardov, ki ne vključujejo odločitev politike, in osnutke predložiti Komisiji. Razviti bi bilo treba regulativne tehnične standarde na področjih obvladovanja tveganj na področju IKT, poročanja o večjih incidentih, povezanih z IKT, testiranja, pa tudi v povezavi s ključnimi zahtevami za dobro spremljanje tveganj tretjih strani na področju IKT. Komisija in evropski nadzorni organi bi morali zagotoviti, da bi lahko te standarde in zahteve vsi finančni subjekti uporabljali sorazmerno glede na njihovo velikost in splošen profil tveganja ter naravo, obseg in kompleksnost njihovih storitev, dejavnosti in poslovanja. Na Komisijo bi bilo treba prenesti pooblastilo za sprejetje teh regulativnih tehničnih standardov z delegiranimi akti na podlagi člena 290 PDEU ter v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

(100) Za lažjo primerljivost poročil o večjih incidentih, povezanih z IKT, in večjih operativnih ali varnostnih incidentih, povezanih s plačili, pa tudi za zagotovitev preglednosti glede pogodbenih dogovorov o uporabi storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT, bi morali evropski nadzorni organi pripraviti osnutke izvedbenih tehničnih standardov, ki bi določali standardizirane predloge, obrazce in postopke, v skladu s katerimi bi finančni subjekti poročali o večjem incidentu, povezanem z IKT, in večjem operativnem ali varnostnem incidentu, povezanem s plačili, ter standardizirane predloge za register informacij. Evropski nadzorni organi bi morali pri oblikovanju teh standardov upoštevati velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja. Na Komisijo bi bilo treba prenesti pooblastilo za sprejetje teh izvedbenih tehničnih standardov z izvedbenimi akti na podlagi člena 291 PDEU ter v skladu s členom 15 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

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

(101) Ker so bile nadaljnje zahteve že določene z delegiranimi in izvedbenimi akti, ki temeljijo na tehničnih regulativnih in izvedbenih tehničnih standardih iz uredb (ES) št. 1060/2009 ([23]), (EU) št. 648/2012 ([24]), (EU) št. 600/2014 ([25]) in (EU) št. 909/2014 ([26]) Evropskega parlamenta in Sveta, je ustrezno pooblastiti evropske nadzorne organe, da bodisi posamično bodisi skupaj prek Skupnega odbora Komisiji predložijo regulativne in izvedbene tehnične standarde za sprejetje delegiranih in izvedbenih aktov, s katerimi se prenašajo in posodabljajo obstoječa pravila o obvladovanju tveganj na področju IKT.

(102) Ker ta uredba, skupaj z Direktivo (EU) 2022/2556 Evropskega parlamenta in Sveta ([27]), pomeni konsolidacijo določb o obvladovanju tveganj na področju IKT iz številnih uredb in direktiv pravnega reda Unije na področju finančnih storitev, vključno z uredbami (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014 ter Uredbo (EU) 2016/1011 Evropskega parlamenta in Sveta ([28]), bi bilo treba za zagotovitev popolne skladnosti navedene uredbe spremeniti, da se razjasni, da so veljavne določbe, povezane s tveganji na področju IKT, določene v tej uredbi.

(103) Zato bi bilo treba področje uporabe zadevnih členov o operativnem tveganju, na podlagi katerih so bili v skladu s pooblastili iz uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 sprejeti delegirani in izvedbeni akti, omejiti z namenom, da se v to uredbo prenesejo vse določbe o vidikih digitalne operativne odpornosti, ki so trenutno del navedenih uredb.

(104) Morebitna sistemska kibernetska tveganja, povezana z uporabo infrastruktur IKT, ki omogočajo delovanje plačilnih sistemov in opravljanje dejavnosti obdelave plačil, bi bilo treba ustrezno obravnavati na ravni Unije s harmoniziranimi pravili o digitalni odpornosti. V ta namen bi morala Komisija hitro oceniti potrebo po pregledu področja uporabe te uredbe, pri čemer se pregled uskladi z izidom celovitega pregleda, predvidenega na podlagi Direktive (EU) 2015/2366. Številni obsežni napadi v zadnjem desetletju dokazujejo, da so plačilni sistemi postali izpostavljeni kibernetskim grožnjam. Plačilni sistemi in dejavnosti obdelave plačil so v središču verige plačilnih storitev in so tesno medsebojno povezani s finančnim sistemom kot celoto, zato so postali ključnega pomena za delovanje finančnih trgov Unije. Kibernetski napadi na take sisteme lahko povzročijo resne operativne motnje poslovanja, ki imajo neposredne posledice za ključne gospodarske funkcije, kot je poenostavitev plačil, in posredne učinke na povezane gospodarske procese. Dokler se na ravni Unije ne vzpostavita harmonizirana ureditev ter nadzor operaterjev plačilnih sistemov in subjektov obdelovalcev, se lahko države članice z namenom uporabljanja podobnih tržnih praks pri uporabi pravil za operaterje plačilnih sistemov in subjekte obdelovalce, ki so nadzorovani v okviru njihove jurisdikcije, zgledujejo po zahtevah glede digitalne operativne odpornosti iz te uredbe.

([23]) Uredba (ES) št. 1060/2009 Evropskega parlamenta in Sveta z dne 16. septembra 2009 o bonitetnih agencijah (UL L 302, 17.11.2009, str. 1).

([24]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).

([25]) Uredba (EU) št. 600/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov in spremembi Uredbe (EU) št. 648/2012 (UL L 173, 12.6.2014, str. 84).

([26]) Uredba (EU) št. 909/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah ter o spremembi direktiv 98/26/ES in 2014/65/EU ter Uredbe (EU) št. 236/2012 (UL L 257, 28.8.2014, str. 1).

([27]) Direktiva (EU) 2022/2556 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o spremembi direktiv 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 in (EU) 2016/2341 glede digitalne operativne odpornosti v finančnem sektorju (glej stran 153 tega Uradnega lista).

([28]) Uredba (EU) 2016/1011 Evropskega parlamenta in Sveta z dne 8. junija 2016 o indeksih, ki se uporabljajo kot referenčne vrednosti v finančnih instrumentih in finančnih pogodbah ali za merjenje uspešnosti investicijskih skladov, in spremembi direktiv 2008/48/ES in 2014/17/EU ter Uredbe (EU) št. 596/2014 (UL L 171, 29.6.2016, str. 1).

(105) Ker cilja te uredbe, in sicer doseganja visoke stopnje digitalne operativne odpornosti regulativnih finančnih subjektov, države članice zaradi potrebe po harmonizaciji več različnih pravil v pravu Unije in nacionalnem pravu ne morejo zadovoljivo doseči, temveč se zaradi obsega in učinkov te uredbe lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(106) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([29]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 10. maja 2021 ([30]) –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

Splošne določbe

Člen 1

Predmet urejanja

1. Za doseganje visoke skupne stopnje digitalne operativne odpornosti ta uredba določa enotne zahteve glede varnosti omrežnih in informacijskih sistemov, ki podpirajo poslovne procese finančnih subjektov, kot sledi:

(a) zahteve, ki veljajo za finančne subjekte glede:

  (i) obvladovanja tveganj na področju informacijske in komunikacijske tehnologije (IKT);

  (ii) poročanja pristojnim organom o večjih incidentih, povezanih z IKT, in prostovoljnega obveščanja pristojnih organov o pomembnih kibernetskih grožnjah;

  (iii) poročanja finančnih subjektov iz člena 2(1), točke (a) do (d), pristojnim organom o večjih operativnih ali varnostnih incidentih, povezanih s plačili;

  (iv) testiranja digitalne operativne odpornosti;

  (v) izmenjave informacij in obveščevalnih podatkov v zvezi s kibernetskimi grožnjami in ranljivostmi;

  (vi) ukrepov za dobro obvladovanje tveganj tretjih strani na področju IKT;

(b) zahteve v zvezi s pogodbenimi dogovori, sklenjenimi med tretjimi ponudniki storitev IKT in finančnimi subjekti;

(c) pravila za vzpostavitev in izvajanje okvira nadzora za ključne tretje ponudnike storitev IKT, ko opravljajo storitve za finančne subjekte;

(d) pravila o sodelovanju med pristojnimi organi in pravila o nadzoru in izvrševanju s strani pristojnih organov v zvezi z vsemi zadevami, zajetimi v tej uredbi.

2. V zvezi s finančnimi subjekti, opredeljenimi kot bistvenimi ali pomembnimi subjekti na podlagi nacionalnih pravil za prenos člena 3 Direktive (EU) 2022/2555, se ta uredba za namene člena 4 navedene direktive šteje za sektorski pravni akt Unije.

3. Ta uredba ne posega v odgovornost držav članic glede temeljnih državnih funkcij v zvezi z javno varnostjo, obrambo in nacionalno varnostjo v skladu s pravom Unije.

([29]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

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

Člen 2

Področje uporabe

1. Ta uredba se brez poseganja v odstavka 3 in 4 uporablja za naslednje subjekte:

(a) kreditne institucije;

(b) plačilne institucije, vključno s plačilnimi institucijami, izvzetimi na podlagi Direktive (EU) 2015/2366;

(c) ponudnike storitev zagotavljanja informacij o računih;

(d) institucije za izdajo elektronskega denarja, vključno z institucijami za izdajo elektronskega denarja, izvzetimi na podlagi Direktive 2009/110/ES;

(e) investicijska podjetja;

(f) ponudnike storitev v zvezi s kriptosredstvi, pooblaščene na podlagi uredbe Evropskega parlamenta in Sveta o trgih kriptosredstev ter spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937 (v nadaljnjem besedilu: uredba o trgih kriptosredstev) in izdajatelje žetonov, vezanih na sredstva;

(g) centralne depotne družbe;

(h) centralne nasprotne stranke;

(i) mesta trgovanja;

(j) repozitorije sklenjenih poslov;

(k) upravitelje alternativnih investicijskih skladov;

(l) družbe za upravljanje;

(m) izvajalce storitev sporočanja podatkov;

(n) zavarovalnice in pozavarovalnice;

(o) zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj;

(p) institucije za poklicno pokojninsko zavarovanje;

(q) bonitetne agencije;

(r) upravljavce ključnih referenčnih vrednosti;

(s) ponudnike storitev množičnega financiranja;

(t) repozitorije listinjenja;

(u) tretje ponudnike storitev IKT.

2. V tej uredbi se subjekti iz odstavka 1, točke (a) do (t), skupaj imenujejo „finančni subjekti“.

3. Ta uredba se ne uporablja za:

(a) upravitelje alternativnih investicijskih skladov iz člena 3(2) Direktive 2011/61/EU;

(b) zavarovalnice in pozavarovalnice iz člena 4 Direktive 2009/138/ES;

(c) institucije za poklicno pokojninsko zavarovanje, ki upravljajo pokojninske načrte, ki skupaj nimajo več kot 15 članov;

(d) fizične ali pravne osebe, izvzete na podlagi členov 2 in 3 Direktive 2014/65/EU;

(e) zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj, ki so mikropodjetja ali mala ali srednja podjetja;

(f) poštne institucije, ki opravljajo storitev brezgotovinskega nakazovanja, iz člena 2(5), točka 3, Direktive 2013/36/EU.

4. Države članice lahko s področja uporabe te uredbe izključijo subjekte iz člena 2(5), točke 4 do 23, Direktive 2013/36/EU, ki se nahajajo na njihovem ozemlju. Kadar država članica uporabi to možnost, o tem in o vseh naknadnih spremembah obvesti Komisijo. Komisija da te informacije javno na voljo na svojem spletnem mestu ali na drug lahko dostopen način.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „digitalna operativna odpornost“ pomeni sposobnost finančnega subjekta, da vzpostavi, zagotavlja in pregleduje svojo operativno celovitost in zanesljivost, tako da neposredno ali posredno z uporabo storitev tretjih ponudnikov storitev IKT zagotovi celoten sklop zmožnosti, povezanih z IKT, ki so potrebne za obravnavo varnosti omrežnih in informacijskih sistemov, ki jih uporablja finančni subjekt in ki omogočajo nadaljnje opravljanje in kakovost finančnih storitev, tudi v primeru motenj;

(2) „omrežni in informacijski sistem“ pomeni omrežni in informacijski sistem, kot je opredeljen v členu 6, točka 1, Direktive (EU) 2022/2555;

(3) „obstoječi sistem IKT“ pomeni sistem IKT, ki je dosegel konec življenjskega cikla (konec življenjske dobe), ki zaradi tehnoloških ali komercialnih razlogov ni primeren za nadgradnje ali popravke oziroma ga njegov ponudnik ali tretji ponudnik storitev IKT ne podpira več, vendar pa se še vedno uporablja in podpira funkcije finančnega subjekta;

(4) „varnost omrežnih in informacijskih sistemov“ pomeni varnost omrežnih in informacijskih sistemov, kot je opredeljena v členu 6, točka 2, Direktive (EU) 2022/2555;

(5) „tveganje na področju IKT“ pomeni vsako razumno določljivo okoliščino v zvezi z uporabo omrežnih in informacijskih sistemov, ki lahko, če se uresniči, ogrozi varnost omrežnih in informacijskih sistemov, vseh orodij ali postopkov, odvisnih od tehnologije, operacij in postopkov ali opravljanja storitev, tako da ima škodljive učinke v digitalnem ali fizičnem okolju;

(6) „informacijsko sredstvo“ pomeni zbirko informacij, oprijemljivih ali neoprijemljivih, ki jih je vredno zavarovati;

(7) „sredstvo IKT“ pomeni programsko ali strojno opremo v omrežnih in informacijskih sistemih, ki jih uporablja finančni subjekt;

(8) „incident, povezan z IKT“ pomeni enkraten dogodek ali vrsto povezanih dogodkov, ki jih finančni subjekt ni predvidel ter ki ogrožajo varnost omrežnih in informacijskih sistemov in škodljivo vplivajo na razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov ali na storitve, ki jih opravlja finančni subjekt;

(9) „operativni ali varnostni incident, povezan s plačili“ pomeni enkraten dogodek ali vrsto povezanih dogodkov, ki jih finančni subjekti iz člena 2(1), točke (a) do (d), niso predvideli, ne glede na to, ali so povezani z IKT ali ne, in ki škodljivo vplivajo na razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov, povezanih s plačili, ali na storitve, povezane s plačili, ki jih opravlja finančni subjekt;

(10) „večji incident, povezan z IKT“ pomeni incident, povezan z IKT, ki ima velik škodljiv vpliv na omrežne in informacijske sisteme, ki podpirajo kritične ali pomembne funkcije finančnega subjekta;

(11) „večji operativni ali varnostni incident, povezan s plačili“ pomeni operativni ali varnostni incident, povezan s plačili, ki ima velik škodljiv vpliv na opravljanje storitve, povezane s plačili;

(12) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kot je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(13) „pomembna kibernetska grožnja“ pomeni kibernetsko grožnjo, katere tehnične značilnosti kažejo na to, da bi lahko povzročila večji incident, povezan z IKT, ali večji operativni ali varnostni incident, povezan s plačili;

(14) „kibernetski napad“ pomeni zlonamerni incident, povezan z IKT, ki ga povzroči akter grožnje, ko poskuša uničiti, razkriti, spremeniti, onemogočiti ali ukrasti sredstvo, pridobiti nepooblaščen dostop do njega ali ga nedovoljeno uporabiti;

(15) „obveščevalni podatki o grožnjah“ pomeni informacije, ki so bile združene, preoblikovane, analizirane, razložene ali obogatene, da bi zagotovile potreben okvir za odločanje ter omogočile ustrezno in zadostno razumevanje, da bi se zmanjšal vpliv incidenta, povezanega z IKT, ali kibernetske grožnje, vključno s tehničnimi podrobnostmi kibernetskega napada ter podatki o odgovornih osebah za napad, njihovem načinu delovanja in motivih;

(16) „ranljivost“ pomeni šibkost, dovzetnost ali napako sredstva, sistema, postopka ali nadzora, ki jo je mogoče izkoristiti;

(17) „penetracijsko testiranje na podlagi analize groženj“ pomeni okvir, ki posnema taktike, tehnike in postopke dejanskih akterjev groženj, za katere se šteje, da predstavljajo resnično kibernetsko grožnjo, in ki zagotavlja nadzorovan, prilagojen in na podlagi obveščevalnih podatkov (rdeča ekipa) oblikovan test ključnih aktivnih produkcijskih sistemov finančnega subjekta;

(18) „tveganje tretjih strani na področju IKT“ pomeni tveganje na področju IKT, ki lahko grozi finančnemu subjektu zaradi njegove uporabe storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT ali njihovi podizvajalci, tudi z dogovori o zunanjem izvajanju;

(19) „tretji ponudnik storitev IKT“ pomeni podjetje, ki opravlja storitve IKT;

(20) „ponudnik storitev IKT znotraj skupine“ pomeni podjetje, ki je del finančne skupine in opravlja predvsem storitve IKT finančnim subjektom v isti skupini ali finančnim subjektom, ki spadajo v isto institucionalno shemo za zaščito vlog, vključno z obvladujočimi in odvisnimi podjetji, podružnicami ali drugimi subjekti, ki so pod skupnim lastništvom ali nadzorom;

(21) „storitve IKT“ pomeni digitalne in podatkovne storitve, ki se prek sistemov IKT neprekinjeno opravljajo za enega ali več notranjih ali zunanjih uporabnikov, vključno s strojno opremo kot storitvijo in storitvami v zvezi s strojno opremo, kar vključuje zagotavljanje tehnične podpore s tem, da ponudnik strojne opreme posodablja programsko ali strojno programsko opremo, razen tradicionalnih analognih telefonskih storitev;

(22) „kritična ali pomembna funkcija“ pomeni funkcijo, katere motnja bi bistveno škodovala finančni uspešnosti finančnega subjekta ali trdnosti ali neprekinjenosti njegovih storitev in dejavnosti, oziroma katere prekinjeno, pomanjkljivo ali neuspešno izvajanje bi bistveno oviralo finančni subjekt, da neprekinjeno izpolnjuje pogoje in obveznosti iz njegovega pooblastila ali druge obveznosti v skladu z veljavnim pravom o finančnih storitvah;

(23) „ključni tretji ponudnik storitev IKT“ pomeni tretjega ponudnika storitev IKT, imenovanega kot ključnega v skladu s členom 31;

(24) „tretji ponudnik storitev IKT s sedežem v tretji državi“ pomeni tretjega ponudnika storitev IKT, ki je pravna oseba s sedežem v tretji državi in ki je sklenil pogodbeni dogovor s finančnim subjektom za opravljanje storitev IKT;

(25) „odvisno podjetje“ pomeni odvisno podjetje v smislu člena 2, točka 10, in člena 22 Direktive 2013/34/EU;

(26) „skupina“ pomeni skupino, kot je opredeljena v členu 2, točka 11, Direktive 2013/34/EU;

(27) „obvladujoče podjetje“ pomeni obvladujoče podjetje v smislu člena 2, točka 9, in člena 22 Direktive 2013/34/EU;

(28) „podizvajalec storitev IKT s sedežem v tretji državi“ pomeni podizvajalca storitev IKT, ki je pravna oseba s sedežem v tretji državi in ki je sklenil pogodbeni dogovor bodisi s tretjim ponudnikom storitev IKT ali tretjim ponudnikom storitev IKT s sedežem v tretji državi;

(29) „tveganje koncentracije na področju IKT“ pomeni izpostavljenost enemu ali več povezanim ključnim tretjim ponudnikom storitev IKT, ki ustvarja določeno stopnjo odvisnosti od takih ponudnikov, tako da lahko nedosegljivost, nezmožnost opravljanja storitev ali druga vrsta izpada takega ponudnika potencialno ogrozi sposobnost finančnega subjekta, da opravlja kritične ali pomembne funkcije, ali pa mu povzroči druge vrste škodljivih učinkov, vključno z velikimi izgubami, oziroma ogrozi finančno stabilnost Unije kot celote;

(30) „upravljalni organ“ pomeni upravljalni organ, kot je opredeljen v členu 4(1), točka 36, Direktive 2014/65/EU, členu 3(1), točka 7, Direktive 2013/36/EU, členu 2(1), točka (s), Direktive 2009/65/ES Evropskega parlamenta in Sveta ([31]), členu 2(1), točka 45, Uredbe (EU) št. 909/2014, členu 3(1), točka 20, Uredbe (EU) 2016/1011, in v ustrezni določbi uredbe o trgih kriptosredstev ali enakovredne osebe, ki dejansko vodijo subjekt ali imajo kritične funkcije v skladu z ustreznim pravom Unije ali nacionalnim pravom;

(31) „kreditna institucija“ pomeni kreditno institucijo, kot je opredeljena v členu 4(1), točka 1, Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta ([32]);

(32) „institucija, izvzeta na podlagi Direktive 2013/36/EU“ pomeni subjekt iz člena 2(5), točke 4 do 23, Direktive 2013/36/EU;

(33) „investicijsko podjetje“ pomeni investicijsko podjetje, kot je opredeljeno v členu 4(1), točka 1, Direktive 2014/65/EU;

(34) „malo in nepovezano investicijsko podjetje“ pomeni investicijsko podjetje, ki izpolnjuje pogoje iz člena 12(1) Uredbe (EU) 2019/2033 Evropskega parlamenta in Sveta ([33]);

(35) „plačilna institucija“ pomeni plačilno institucijo, kot je opredeljena v členu 4, točka 4, Direktive (EU) 2015/2366;

(36) „plačilna institucija, izvzeta na podlagi Direktive (EU) 2015/2366“ pomeni plačilno institucijo, ki je izvzeta na podlagi člena 32(1) Direktive (EU) 2015/2366;

(37) „ponudnik storitev zagotavljanja informacij o računih“ pomeni ponudnika storitev zagotavljanja informacij o računih iz člena 33(1) Direktive (EU) 2015/2366;

(38) „institucija za izdajo elektronskega denarja“ pomeni institucijo za izdajo elektronskega denarja, kot je opredeljena v členu 2, točka 1, Direktive 2009/110/ES Evropskega parlamenta in Sveta;

(39) „institucija za izdajo elektronskega denarja, izvzeta na podlagi Direktive 2009/110/ES“ pomeni institucijo za izdajo elektronskega denarja, ki ji je bila odobrena opustitev iz člena 9(1) Direktive 2009/110/ES;

(40) „centralna nasprotna stranka“ pomeni centralno nasprotno stranko, kot je opredeljena v členu 2, točka 1, Uredbe (EU) št. 648/2012;

(41) „repozitorij sklenjenih poslov“ pomeni repozitorij sklenjenih poslov, kot je opredeljen v členu 2, točka 2, Uredbe (EU) št. 648/2012;

(42) „centralna depotna družba“ pomeni centralno depotno družbo, kot je opredeljena v členu 2(1), točka 1, Uredbe (EU) št. 909/2014;

(43) „mesto trgovanja“ pomeni mesto trgovanja, kot je opredeljeno v členu 4(1), točka 24, Direktive 2014/65/EU;

(44) „upravitelj alternativnih investicijskih skladov“ pomeni upravitelja alternativnih investicijskih skladov, kot je opredeljen v členu 4(1), točka (b), Direktive 2011/61/EU;

(45) „družba za upravljanje“ pomeni družbo za upravljanje, kot je opredeljena v členu 2(1), točka (b), Direktive 2009/65/ES;

(46) „izvajalec storitev sporočanja podatkov“ pomeni izvajalca storitev sporočanja podatkov v smislu Uredbe (EU) št. 600/2014, iz člena 2(1), točke 34 do 36 navedene uredbe;

(47) „zavarovalnica“ pomeni zavarovalnico, kot je opredeljena v členu 13, točka 1, Direktive 2009/138/ES;

(48) „pozavarovalnica“ pomeni pozavarovalnico, kot je opredeljena v členu 13, točka 4, Direktive 2009/138/ES;

([31]) Direktiva 2009/65/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o usklajevanju zakonov in drugih predpisov o kolektivnih naložbenih podjemih za vlaganja v prenosljive vrednostne papirje (KNPVP) (UL L 302, 17.11.2009, str. 32).

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

([33]) Uredba (EU) 2019/2033 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o bonitetnih zahtevah za investicijska podjetja ter o spremembi uredb (EU) št. 1093/2010, (EU) št. 575/2013, (EU) št. 600/2014 in (EU) št. 806/2014 (UL L 314, 5.12.2019, str. 1).

(49) „zavarovalni posrednik“ pomeni zavarovalnega posrednika, kot je opredeljen v členu 2(1), točka 3, Direktive (EU) 2016/97 Evropskega parlamenta in Sveta ([34]);

(50) „posrednik dopolnilnih zavarovanj“ pomeni posrednika dopolnilnih zavarovanj, kot je opredeljen v členu 2(1), točka 4, Direktive (EU) 2016/97;

(51) „pozavarovalni posrednik“ pomeni pozavarovalnega posrednika, kot je opredeljen v členu 2(1), točka 5, Direktive (EU) 2016/97;

(52) „institucija za poklicno pokojninsko zavarovanje“ pomeni institucijo za poklicno pokojninsko zavarovanje, kot je opredeljena v členu 6, točka 1, Direktive (EU) 2016/2341;

(53) „mala institucija za poklicno pokojninsko zavarovanje“ pomeni institucijo za poklicno pokojninsko zavarovanje, ki upravlja pokojninske načrte, ki imajo skupaj manj kot 100 članov;

(54) „bonitetna agencija“ pomeni bonitetno agencijo, kot je opredeljena v členu 3(1), točka (b), Uredbe (ES) št. 1060/2009;

(55) „ponudnik storitev v zvezi s kriptosredstvi“ pomeni ponudnika storitev v zvezi s kriptosredstvi, kot je opredeljen v ustrezni določbi uredbe o trgih kriptosredstev;

(56) „izdajatelj žetonov, vezanih na sredstva“ pomeni izdajatelja žetonov, vezanih na sredstva, kot so opredeljeni v ustrezni določbi uredbe o trgih kriptosredstev;

(57) „upravljavec ključnih referenčnih vrednosti“ pomeni upravljavca ključnih referenčnih vrednosti, kot so opredeljene v členu 3(1), točka 25, Uredbe (EU) 2016/1011;

(58) „ponudnik storitev množičnega financiranja“ pomeni ponudnika storitev množičnega financiranja, kot je opredeljen v členu 2(1), točka (e), Uredbe (EU) 2020/1503 Evropskega parlamenta in Sveta ([35]);

(59) „repozitorij listinjenj“ pomeni repozitorij listinjenj, kot je opredeljen v členu 2, točka 23, Uredbe (EU) 2017/2402 Evropskega parlamenta in Sveta ([36]);

(60) „mikropodjetje“ pomeni finančni subjekt, ki ni mesto trgovanja, centralna nasprotna stranka, repozitorij sklenjenih poslov ali centralna depotna družba, ki ima manj kot 10 zaposlenih in ima letni promet in/ali letno bilančno vsoto, ki ne presega 2 milijonov EUR;

(61) „glavni nadzornik“ pomeni evropski nadzorni organ, imenovan v skladu s členom 31(1), točka (b), te uredbe;

(62) „Skupni odbor“ pomeni odbor iz člena 54 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010;

(63) „malo podjetje“ pomeni finančni subjekt, ki ima 10 ali več, vendar manj kot 50 zaposlenih in ima letni promet in/ali letno bilančno vsoto, ki presega 2 milijona, vendar ne presega 10 milijonov EUR;

(64) „srednje podjetje“ pomeni finančni subjekt, ki ni malo podjetje in ima manj kot 250 zaposlenih ter ima letni promet, ki ne presega 50 milijonov EUR, in/ali letno bilančno vsoto, ki ne presega 43 milijonov EUR;

(65) „javni organ“ pomeni vsak vladni organ ali drug subjekt javne uprave, vključno z nacionalnimi centralnimi bankami.

([34]) Direktiva (EU) 2016/97 Evropskega parlamenta in Sveta z dne 20. januarja 2016 o distribuciji zavarovalnih produktov (UL L 26, 2.2.2016, str. 19).

([35]) Uredba (EU) 2020/1503 Evropskega parlamenta in Sveta z dne 7. oktobra 2020 o evropskih ponudnikih storitev množičnega financiranja za podjetnike ter spremembi Uredbe (EU) 2017/1129 in Direktive (EU) 2019/1937 (UL L 347, 20.10.2020, str. 1).

([36]) Uredba (EU) 2017/2402 Evropskega parlamenta in Sveta z dne 12. decembra 2017 o določitvi splošnega okvira za listinjenje in o vzpostavitvi posebnega okvira za enostavno, pregledno in standardizirano listinjenje ter o spremembah direktiv 2009/65/ES, 2009/138/ES in 2011/61/EU ter uredb (ES) št. 1060/2009 in (EU) št. 648/2012 (UL L 347, 28.12.2017, str. 35).

Člen 4

Načelo sorazmernosti

1. Finančni subjekti izvajajo pravila iz poglavja II v skladu z načelom sorazmernosti, pri tem pa upoštevajo svojo velikost in splošni profil tveganja ter naravo, obseg in kompleksnost svojih storitev, dejavnosti in poslovanja.

2. Poleg tega finančni subjekti uporabljajo poglavja III, IV in V, oddelek I, sorazmerno s svojo velikostjo in splošnim profilom tveganja ter naravo, obsegom in kompleksnostjo svojih storitev, dejavnosti in poslovanja, kot je posebej določeno v ustreznih pravilih iz navedenih poglavij.

3. Pristojni organi pri pregledu skladnosti okvira za obvladovanje tveganj na področju IKT na podlagi poročil, predloženih na zahtevo pristojnih organov na podlagi člena 6(5) in člena 16(2), preučijo, ali finančni subjekti uporabljajo načelo sorazmernosti.

POGLAVJE II

Obvladovanje tveganj na področju IKT

Oddelek I

Člen 5

Upravljanje in organizacija

1. Finančni subjekti vzpostavijo okvir notranjega upravljanja in nadzora, ki zagotavlja učinkovito in skrbno obvladovanje tveganj na področju IKT v skladu s členom 6(4), da bi se dosegla visoka raven digitalne operativne odpornosti.

2. Upravljalni organ finančnega subjekta opredeli, odobri in nadzira izvajanje vseh dogovorov, povezanih z okvirom za obvladovanje tveganj na področju IKT iz člena 6(1), in je odgovoren zanj.

Za potrebe prvega pododstavka upravljalni organ:

(a) nosi končno odgovornost za obvladovanje tveganj na področju IKT, s katerimi se sooča finančni subjekt;

(b) uvede politike, katerih cilj je zagotoviti ohranjanje visokih standardov razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov;

(c) določi jasne vloge in odgovornosti za vse funkcije, povezane z IKT, in vzpostavi ustrezno ureditev upravljanja, da se zagotovijo učinkovita in pravočasna komunikacija, sodelovanje in usklajevanje med temi funkcijami;

(d) nosi splošno odgovornost za določitev in odobritev strategije za digitalno operativno odpornost iz člena 6(8), vključno z določitvijo ustrezne tolerančne ravni tveganja na področju IKT za finančni subjekt, kot je navedeno v členu 6(8), točka (b);

(e) odobri, nadzira in redno pregleduje izvajanje politike neprekinjenega poslovanja na področju IKT in načrtov odzivanja in okrevanja IKT iz člena 11(1) oziroma (3), ki se lahko sprejmejo kot namenska posebna politika in kot sestavni del subjektove splošne politike neprekinjenega poslovanja ter načrta odzivanja in okrevanja;

(f) odobri in redno pregleduje notranje revizijske načrte finančnega subjekta na področju IKT, revizije na področju IKT in njihove bistvene spremembe;

(g) dodeli in občasno pregleda ustrezni proračun, da lahko finančni subjekt izpolnjuje potrebe po digitalni operativni odpornosti v zvezi z vsemi vrstami virov, vključno z ustreznimi programi ozaveščanja o varnosti IKT in usposabljanjem o digitalni operativni odpornosti iz člena 13(6) ter veščinami na področju IKT za vse zaposlene;

(h) odobri in redno pregleduje politiko finančnega subjekta glede dogovorov o uporabi storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT;

(i) na ravni podjetja vzpostavi kanale poročanja, da je ustrezno obveščen o naslednjem:

(i) dogovorih o uporabi storitev IKT, sklenjenih s tretjimi ponudniki storitev IKT;

(ii) vseh ustreznih načrtovanih pomembnih spremembah v zvezi s tretjimi ponudniki storitev IKT;

(iii) možnem učinku takih sprememb na kritične ali pomembne funkcije, za katere veljajo navedeni dogovori, vključno s povzetkom analize tveganja za oceno učinka teh sprememb, ter vsaj o večjih incidentih, povezanih z IKT, in njihovem učinku ter o odzivnih, sanacijskih in popravnih ukrepih.

3. Finančni subjekti, ki niso mikropodjetja, določijo vlogo za spremljanje dogovorov, sklenjenih s tretjimi ponudniki storitev IKT o uporabi storitev IKT, ali določijo člana višjega vodstva, ki bo odgovoren za nadzor s tem povezane izpostavljenosti tveganju in ustrezne dokumentacije.

4. Člani upravljalnega organa finančnega subjekta dejavno obnavljajo zadostno znanje in spretnosti, da lahko razumejo in ocenijo tveganje na področju IKT ter njegov učinek na poslovanje finančnega subjekta, tudi z rednim namenskim usposabljanjem, primernim za tveganje na področju IKT, ki ga je treba obvladovati.

Oddelek II

Člen 6

Okvir za obvladovanje tveganj na področju IKT

1. Finančni subjekti morajo imeti trden, celovit in dobro dokumentiran okvir za obvladovanje tveganj na področju IKT, ki je del njihovega splošnega sistema obvladovanja tveganj in jim omogoča hitro, učinkovito in celovito obravnavo tveganj na področju IKT ter zagotavljanje visoke stopnje digitalne operativne odpornosti.

2. Okvir za obvladovanje tveganj na področju IKT vključuje najmanj strategije, politike, postopke, protokole in orodja IKT, ki so potrebni za pravilno in ustrezno zaščito vseh informacijskih sredstev in sredstev IKT, vključno z računalniško programsko opremo, strojno opremo in strežniki, ter za zaščito vseh ustreznih fizičnih komponent in infrastrukture, kot so prostori, podatkovni centri in občutljiva namenska območja, za zagotovitev, da so vsa informacijska sredstva in sredstva IKT ustrezno zaščitena pred tveganji, vključno s škodo in nepooblaščenim dostopom ali nedovoljeno uporabo.

3. Finančni subjekti v skladu s svojim okvirom za obvladovanje tveganj na področju IKT zmanjšujejo vpliv tveganja na področju IKT z uporabo ustreznih strategij, politik, postopkov, protokolov in orodij IKT. Pristojnim organom na njihovo zahtevo zagotavljajo popolne in posodobljene informacije o tveganjih na področju IKT in o svojem okviru za obvladovanje tveganj na področju IKT.

4. Finančni subjekti, ki niso mikropodjetja, odgovornost za obvladovanje tveganj na področju IKT in nadzor nad njimi dodelijo nadzorni funkciji in poskrbijo, da ima taka nadzorna funkcija ustrezno raven neodvisnosti, da se preprečijo nasprotja interesov. Finančni subjekti zagotovijo ustrezno ločitev in neodvisnost funkcij obvladovanja tveganj na področju IKT, nadzornih funkcij in funkcij notranje revizije v skladu z modelom treh obrambnih linij ali internim modelom upravljanja in obvladovanja tveganj.

5. Okvir za obvladovanje tveganj na področju IKT se dokumentira in pregleda najmanj enkrat letno oziroma redno za mikropodjetja, pa tudi ob pojavu večjih incidentov, povezanih z IKT, in ob upoštevanju nadzornih navodil ali sklepov, ki izhajajo iz ustreznih postopkov testiranja ali revizije digitalne operativne odpornosti. Nenehno se izboljšuje na podlagi izkušenj, pridobljenih pri izvajanju in spremljanju. Poročilo o pregledu okvira za obvladovanje tveganj na področju IKT se posreduje pristojnemu organu na njegovo zahtevo.

6. Okvir za obvladovanje tveganj na področju IKT finančnih subjektov, ki niso mikropodjetja, je redno predmet notranje revizije revizorjev v skladu z revizijskim načrtom finančnih subjektov. Ti revizorji morajo imeti zadostno znanje, spretnosti in strokovno znanje v zvezi s tveganji na področju IKT, kot tudi ustrezno neodvisnost. Pogostost in osredotočenost revizij na področju IKT morata biti sorazmerni s tveganjem na področju IKT, s katerim se sooča finančni subjekt.

7. Finančni subjekti na podlagi sklepov notranjega revizijskega pregleda vzpostavijo formalni postopek spremljanja, vključno s pravili za pravočasno preverjanje in sanacijo na podlagi ključnih ugotovitev revizij na področju IKT.

8. Okvir za obvladovanje tveganj na področju IKT vključuje strategijo za digitalno operativno odpornost, ki določa, kako se okvir izvaja. V ta namen strategija za digitalno operativno odpornost vključuje metode za obravnavanje tveganj na področju IKT in doseganje določenih ciljev na področju IKT, tako da:

(a) pojasnjuje, kako okvir za obvladovanje tveganj na področju IKT podpira poslovno strategijo in cilje finančnega subjekta;

(b) določa tolerančno raven tveganja na področju IKT v skladu z nagnjenostjo finančnega subjekta k prevzemanju tveganja in analizira toleranco učinka za motnje na področju IKT;

(c) določa jasne cilje glede informacijske varnosti, tudi ključne kazalnike uspešnosti in ključne metrike tveganja;

(d) pojasnjuje referenčno arhitekturo IKT in vse spremembe, potrebne za dosego določenih poslovnih ciljev;

(e) opisuje različne mehanizme, vzpostavljene za odkrivanje, varovanje in preprečevanje učinkov incidentov, povezanih z IKT;

(f) dokumentira trenutno stanje digitalne operativne odpornosti na podlagi števila prijavljenih večjih incidentov, povezanih z IKT, in učinkovitosti preventivnih ukrepov;

(g) izvaja testiranje digitalne operativne odpornosti v skladu s poglavjem IV te uredbe;

(h) opisuje komunikacijske strategije v primeru incidentov, povezanih z IKT, ki jih je treba razkriti v skladu s členom 14.

9. Finančni subjekti lahko v okviru strategije za digitalno operativno odpornost iz odstavka 8 opredelijo celostno večdobaviteljsko strategijo za IKT na ravni skupine ali subjekta, ki prikazuje ključne odvisnosti od tretjih ponudnikov storitev IKT in pojasnjuje razloge za uporabo različnih tretjih ponudnikov storitev IKT.

10. Finančni subjekti lahko v skladu s sektorskim pravom Unije in nacionalnim sektorskim pravom naloge preverjanja skladnosti z zahtevami glede obvladovanja tveganj na področju IKT oddajo v zunanje izvajanje podjetjem znotraj skupine ali zunanjim podjetjem. V primerih tovrstnega zunanjega izvajanja finančni subjekt ostane v celoti odgovoren za preverjanje skladnosti z zahtevami glede obvladovanja tveganj na področju IKT.

Člen 7

Sistemi, protokoli in orodja IKT

Finančni subjekti za reševanje in obvladovanje tveganj na področju IKT uporabljajo in vzdržujejo posodobljene sisteme, protokole in orodja IKT, ki so:

(a) ustrezni glede na obsežnost operacij, ki podpirajo izvajanje njihovih dejavnosti, v skladu z načelom sorazmernosti iz člena 4;

(b) zanesljivi;

(c) opremljeni z zadostno zmogljivostjo, da pravilno obdelajo podatke, potrebne za izvajanje dejavnosti in pravočasno opravljanje storitev, ter po potrebi obravnavajo velike količine naročil, sporočil ali poslov, tudi kadar se uvede nova tehnologija;

(d) tehnološko odporni, da se ustrezno spopadajo s potrebami po obdelavi dodatnih informacij, kot se zahteva v stresnih tržnih razmerah ali drugih neugodnih razmerah.

Člen 8

Identificiranje

1. Finančni subjekti v sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) identificirajo, razvrstijo in ustrezno dokumentirajo vse poslovne funkcije, vloge in odgovornosti, ki jih podpirajo IKT, informacijska sredstva in sredstva IKT, ki podpirajo te funkcije, ter njihove vloge in odvisnosti v povezavi s tveganjem na področju IKT. Finančni subjekti po potrebi in vsaj enkrat letno pregledajo ustreznost te razvrstitve in vse ustrezne dokumentacije.

2. Finančni subjekti stalno identificirajo vse vire tveganja na področju IKT, zlasti izpostavljenost tveganju, ki ogroža druge finančne subjekte ali pa ga ti povzročajo, ter ocenjujejo kibernetske grožnje in ranljivosti na področju IKT, pomembne za njihove poslovne funkcije, ki jih podpirajo IKT, ter informacijska sredstva in sredstva IKT. Finančni subjekti redno oziroma vsaj enkrat letno pregledujejo scenarije tveganj, ki vplivajo nanje.

3. Finančni subjekti, ki niso mikropodjetja, izvedejo oceno tveganja ob vsaki večji spremembi infrastrukture omrežnega in informacijskega sistema ter procesov ali postopkov, ki vplivajo na njihove funkcije, ki jih podpirajo IKT, ter informacijska sredstva ali sredstva IKT.

4. Finančni subjekti identificirajo vsa informacijska sredstva in sredstva IKT, vključno s tistimi na oddaljenih lokacijah, omrežne vire in strojno opremo ter popišejo tiste, ki se štejejo za ključne. Popišejo konfiguracijo informacijskih sredstev in sredstev IKT ter povezave in soodvisnosti med različnimi informacijskimi sredstvi in sredstvi IKT.

5. Finančni subjekti identificirajo in dokumentirajo vse postopke, ki so odvisni od tretjih ponudnikov storitev IKT, in identificirajo medsebojne povezave s tretjimi ponudniki storitev IKT, ki opravljajo storitve, ki podpirajo kritične ali pomembne funkcije.

6. Finančni subjekti za namene odstavkov 1, 4 in 5 vzdržujejo ustrezne evidence in jih posodabljajo redno in ob vsaki večji spremembi iz odstavka 3.

7. Finančni subjekti, ki niso mikropodjetja, redno oziroma vsaj enkrat letno izvajajo posebno oceno tveganja na področju IKT za vse obstoječe sisteme IKT, v vsakem primeru pa pred povezovanjem tehnologij, aplikacij ali sistemov in po njem.

Člen 9

Varovanje in preprečevanje

1. Za namene ustrezne zaščite sistemov IKT in z namenom organiziranja odzivnih ukrepov finančni subjekti stalno spremljajo in nadzirajo varnost in delovanje sistemov in orodij IKT ter z uporabo ustreznih varnostnih orodij, politik in postopkov na področju IKT na najmanjšo možno mero zmanjšujejo učinek tveganj na področju IKT na IKT sisteme.

2. Finančni subjekti oblikujejo, pridobijo in izvajajo varnostne strategije, politike, postopke, protokole in orodja na področju IKT, katerih cilj je zagotoviti odpornost, neprekinjenost in razpoložljivost sistemov IKT, zlasti tistih, ki podpirajo kritične ali pomembne funkcije, ter ohraniti visoke standarde razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov bodisi v mirovanju, uporabi ali med prenosom.

3. Za doseganje ciljev iz odstavka 2 finančni subjekti uporabljajo rešitve in postopke IKT, ki so ustrezni v skladu s členom 4. Te rešitve in postopki IKT:

(a) zagotavljajo varnost sredstev za prenos podatkov;

(b) na najmanjšo možno raven zmanjšujejo tveganje za okvaro ali izgubo podatkov, nepooblaščen dostop in tehnične napake, ki bi lahko oviralo poslovno dejavnost;

(c) preprečujejo pomanjkanje razpoložljivosti, škodovanje avtentičnosti in celovitosti, kršitve zaupnosti in izgubo podatkov;

(d) zagotavljajo, da so podatki zaščiteni pred tveganji, ki nastajajo pri upravljanju podatkov, vključno s slabim upravljanjem, tveganji, povezanimi z obdelavo, in človeškimi napakami.

4. V sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) finančni subjekti:

(a) oblikujejo in dokumentirajo politiko informacijske varnosti, ki določa pravila za zaščito razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov, informacijskih sredstev in sredstev IKT, po potrebi tudi tistih, ki pripadajo njihovim strankam;

(b) v skladu s pristopom, ki temelji na tveganju, vzpostavijo zanesljivo upravljanje omrežja in infrastrukture z uporabo ustreznih tehnik, metod in protokolov, ki lahko vključujejo izvajanje avtomatiziranih mehanizmov za izolacijo prizadetih informacijskih sredstev v primeru kibernetskih napadov;

(c) izvajajo politike, ki omejujejo fizični ali logični dostop do informacijskih sredstev in sredstev IKT do tega, kar je potrebno zgolj za zakonite in odobrene funkcije in dejavnosti, ter v ta namen vzpostavijo sklop politik, postopkov in kontrol, ki obravnavajo pravice dostopa in zagotavljajo njihovo dobro upravljanje;

(d) izvajajo politike in protokole za močne mehanizme avtentikacije, ki temeljijo na ustreznih standardih in namenskih nadzornih sistemih, in zaščitne ukrepe kriptografskih ključev, pri čemer se podatki šifrirajo na podlagi rezultatov odobrenih postopkov za razvrščanje podatkov in oceno tveganj na področju IKT;

(e) izvajajo dokumentirane politike, postopke in kontrole za upravljanje sprememb na področju IKT, vključno s spremembami komponent programske opreme, strojne opreme, strojne programske opreme ter sistemskih ali varnostnih parametrov, ki temeljijo na pristopu ocene tveganja in so sestavni del celotnega postopka finančnega subjekta za upravljanje sprememb, za zagotovitev, da se vse spremembe sistemov IKT nadzorovano evidentirajo, testirajo, ocenijo, odobrijo, izvajajo in preverijo;

(f) imajo ustrezne in celovite dokumentirane politike za popravke in posodobitve.

Za namene prvega pododstavka, točka (b), finančni subjekti infrastrukturo omrežnih povezav načrtujejo na način, ki omogoča takojšnjo prekinitev ali segmentacijo, da se zmanjša na najmanjšo možno mero in prepreči širjenje negativnih učinkov, zlasti za medsebojno povezane finančne postopke.

Za namene prvega pododstavka, točka (e), postopek upravljanja sprememb na področju IKT odobrijo ustrezne ravni vodstva, pri čemer mora imeti ta postopek posebne protokole.

Člen 10

Odkrivanje

1. Finančni subjekti vzpostavijo mehanizme za takojšnje odkrivanje neobičajnega ravnanja v skladu s členom 17, vključno s težavami v zvezi z zmogljivostjo omrežja IKT in incidenti, povezanimi z IKT, ter za identifikacijo morebitnih pomembnih kritičnih točk odpovedi.

Vsi mehanizmi odkrivanja iz prvega pododstavka se redno testirajo v skladu s členom 25.

2. Mehanizmi odkrivanja iz odstavka 1 omogočajo več ravni nadzora, določajo mejne vrednosti opozarjanja in merila za sprožitev in začetek izvajanja postopkov odzivanja na incidente, povezane z IKT, vključno s samodejnimi mehanizmi opozarjanja za ustrezne zaposlene, odgovorne za odzivanje na incidente, povezane z IKT.

3. Finančni subjekti namenijo zadostna sredstva in zmožnosti za spremljanje dejavnosti uporabnikov, pojavov nepravilnosti na področju IKT in incidentov, povezanih z IKT, zlasti kibernetskih napadov.

4. Poleg tega izvajalci storitev sporočanja podatkov vzpostavijo sisteme, s katerimi lahko učinkovito preverijo popolnost poročil o trgovanju, identificirajo izpuste in očitne napake ter zahtevajo ponovni prenos teh poročil.

Člen 11

Odzivanje in okrevanje

1. V sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) in na podlagi zahtev glede identificiranja iz člena 8 finančni subjekti vzpostavijo celovito politiko neprekinjenega poslovanja na področju IKT, ki jo lahko sprejmejo kot namensko posebno politiko, ki je sestavni del splošne politike neprekinjenega poslovanja finančnega subjekta.

2. Finančni subjekti izvajajo politiko neprekinjenega poslovanja na področju IKT z namenskimi, ustreznimi in dokumentiranimi dogovori, načrti, postopki in mehanizmi, katerih cilj je:

(a) zagotoviti neprekinjenost kritičnih ali pomembnih funkcij finančnega subjekta;

(b) hitro, ustrezno in učinkovito odzvati se na vse incidente, povezane z IKT, ter jih odpraviti na način, ki omejuje škodo in daje prednost nadaljevanju dejavnosti in sanacijskim ukrepom;

(c) brez odlašanja aktivirati namenske načrte, ki omogočajo zajezitvene ukrepe, postopke in tehnologije, primerne za vse vrste incidentov, povezanih z IKT, in preprečiti nadaljnjo škodo, ter prilagojene postopke odzivanja in okrevanja, določene v skladu s členom 12;

(d) oceniti predhodne učinke, škodo in izgube;

(e) določiti komunikacijske ukrepe in ukrepe za obvladovanje kriz, ki zagotavljajo, da se posodobljene informacije posredujejo vsem ustreznim internim zaposlenim in zunanjim deležnikom v skladu s členom 14, ter poročati pristojnim organom v skladu s členom 19.

3. V sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) finančni subjekti izvajajo povezane načrte odzivanja in okrevanja IKT, ki so v primeru finančnih subjektov, ki niso mikropodjetja, predmet neodvisnih notranjih revizijskih pregledov.

4. Finančni subjekti vzpostavijo, vzdržujejo in redno testirajo ustrezne načrte neprekinjenega poslovanja na področju IKT, zlasti v zvezi s kritičnimi ali pomembnimi funkcijami, oddanimi v zunanje izvajanje ali zagotovljenimi z dogovori s tretjimi ponudniki storitev IKT.

5. Finančni subjekti v okviru splošne politike neprekinjenega poslovanja izvedejo analizo vpliva na poslovanje zaradi svoje izpostavljenosti resnim motnjam poslovanja. V okviru analize vpliva na poslovanje finančni subjekti ocenijo potencialni vpliv resnih motenj poslovanja, in sicer na podlagi kvantitativnih in kvalitativnih meril, pri čemer po potrebi uporabijo notranje in zunanje podatke in analizo scenarijev. V analizi vpliva na poslovanje se upošteva kritičnost identificiranih in popisanih poslovnih funkcij, podpornih procesov, odvisnosti od tretjih strani in informacijskih sredstev ter njihove medsebojne odvisnosti. Finančni subjekti zagotovijo, da so sredstva IKT in storitve IKT zasnovani in uporabljeni popolnoma v skladu z analizo vpliva na poslovanje, zlasti kar zadeva ustrezno zagotavljanje redundantnosti vseh kritičnih komponent.

6. V sklopu celovitega obvladovanja tveganj na področju IKT finančni subjekti:

(a) testirajo načrte neprekinjenega poslovanja na področju IKT ter načrte odzivanja in okrevanja IKT v povezavi s sistemi IKT, ki podpirajo vse funkcije, vsaj enkrat letno, pa tudi v primeru kakršnih koli bistvenih sprememb sistemov IKT, ki podpirajo kritične ali pomembne funkcije;

(b) testirajo načrte obveščanja o kriznih razmerah, vzpostavljene v skladu s členom 14.

Za namene prvega pododstavka, točka (a), finančni subjekti, ki niso mikropodjetja, v načrte testiranja vključijo scenarije kibernetskih napadov in preklopov med primarno infrastrukturo IKT in redundatno zmogljivostjo, rezervnimi sistemi in redundantnimi obrati, potrebnimi za izpolnitev obveznosti iz člena 12.

Finančni subjekti redno pregledujejo svojo politiko neprekinjenega poslovanja na področju IKT ter načrte odzivanja in okrevanja IKT, pri čemer upoštevajo rezultate testov, izvedenih v skladu s prvim pododstavkom, in priporočila, ki izhajajo iz revizijskih ali nadzornih pregledov.

7. Finančni subjekti, ki niso mikropodjetja, imajo funkcijo obvladovanja kriz, ki v primeru aktiviranja njihovih načrtov neprekinjenega poslovanja na področju IKT ali načrtov odzivanja in okrevanja IKT med drugim določa jasne postopke za upravljanje notranjih in zunanjih obvestil o kriznih razmerah v skladu s členom 14.

8. Finančni subjekti vodijo lahko dostopne evidence o dejavnostih pred motnjami in med njimi, ko se aktivirajo njihovi načrti neprekinjenega poslovanja na področju IKT ter načrti odzivanja in okrevanja IKT.

9. Centralne depotne družbe pristojnim organom predložijo kopije rezultatov testov neprekinjenega poslovanja na področju IKT ali podobnih dejavnosti.

10. Finančni subjekti, ki niso mikropodjetja, pristojnim organom na njihovo zahtevo poročajo o oceni skupnih letnih stroškov in izgub, ki nastanejo zaradi večjih incidentov, povezanih z IKT.

11. Evropski nadzorni organi v skladu s členom 16 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 prek Skupnega odbora do 17. julija 2024 pripravijo skupne smernice za oceno skupnih letnih stroškov in izgub iz odstavka 10.

Člen 12

Politike in postopki varnostnega kopiranja ter postopki in metode obnovitve in okrevanja

1. Da bi se zagotovila obnovitev sistemov in podatkov IKT z minimalnimi izpadi, omejenimi motnjami in izgubami, finančni subjekti v sklopu okvira za obvladovanje tveganj na področju IKT razvijejo in dokumentirajo:

(a) politike in postopke varnostnega kopiranja, ki določajo obseg podatkov za varnostno kopiranje in najmanjšo pogostost varnostnega kopiranja na podlagi kritičnosti informacij ali stopnje zaupnosti podatkov;

(b) postopke in metode obnovitve in okrevanja.

2. Finančni subjekti vzpostavijo sisteme za varnostno kopiranje, ki se lahko aktivirajo v skladu s politikami in postopki varnostnega kopiranja ter postopki in metodami obnovitve in okrevanja. Aktivacija sistemov za varnostno kopiranje ne sme ogrožati varnosti omrežnih in informacijskih sistemov oziroma razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti podatkov. Postopki varnostnega kopiranja ter postopki in metode obnovitve in okrevanja se redno testirajo.

3. Finančni subjekti pri obnavljanju varnostnih kopij podatkov z lastnimi sistemi uporabljajo sisteme IKT, ki so fizično in logično ločeni od izvornega sistema IKT. Sistemi IKT so varno zaščiteni pred nepooblaščenim dostopom ali okvarami na področju IKT in omogočajo pravočasno obnovitev storitev, po potrebi z uporabo varnostnih kopij podatkov in sistemov.

Za centralne nasprotne stranke morajo načrti okrevanja zagotoviti obnovitev vseh transakcij, ki so bile v teku v času motnje, s čimer bo centralni nasprotni stranki omogočeno zanesljivo nadaljnje delovanje in dokončanje poravnave na predvideni datum.

Izvajalci storitev sporočanja podatkov poleg tega vzdržujejo zadostna sredstva ter imajo zmogljivosti za varnostno kopiranje in obnovitev, da lahko vedno nudijo in vzdržujejo svoje storitve.

4. Finančni subjekti, ki niso mikropodjetja, vzdržujejo redundantne zmogljivosti IKT, opremljene z viri, zmožnostmi in funkcijami, ki so ustrezne za zagotavljanje poslovnih potreb. Mikropodjetja na podlagi svojega profila tveganja ocenijo potrebo po ohranjanju takih redundantnih zmogljivosti IKT.

5. Centralne depotne družbe ohranjajo vsaj eno sekundarno lokacijo za obdelavo z ustreznimi viri, zmožnostmi, funkcijami in kadrovsko ureditvijo za zagotavljanje poslovnih potreb.

Sekundarna lokacija za obdelavo:

(a) je na zadostni geografski razdalji od primarne lokacije za obdelavo, da se zagotovi, da ima drugačen profil tveganja, in prepreči, da bi jo prizadel dogodek, ki je prizadel primarno lokacijo;

(b) je zmožna zagotoviti enako neprekinjenost kritičnih ali pomembnih funkcij kot na primarni lokaciji ali zagotoviti raven storitev, potrebnih za zagotovitev, da finančni subjekt opravlja svoje kritične operacije v okviru ciljev obnovitve;

(c) je takoj dostopna zaposlenim pri finančnem subjektu, da se zagotovi neprekinjenost kritičnih ali pomembnih funkcij, če primarna lokacija za obdelavo postane nedostopna.

6. Finančni subjekti pri določanju ciljev glede časa in okrevanja točk obnovitve za vsako funkcijo upoštevajo, ali gre za kritično ali pomembno funkcijo in potencialni splošni učinek na učinkovitost trga. Taki cilji glede časa zagotavljajo, da so v skrajnih scenarijih dosežene dogovorjene ravni storitev.

7. Finančni subjekti med obnovitvijo po incidentu, povezanem z IKT, opravijo potrebna preverjanja, vključno z večkratnimi pregledi in postopki usklajevanja, da se ohrani najvišja raven celovitosti podatkov. Ta preverjanja se opravijo tudi pri rekonstrukciji podatkov zunanjih deležnikov, da se zagotovi skladnost vseh podatkov med sistemi.

Člen 13

Učenje in razvoj

1. Finančni subjekti imajo vzpostavljene zmožnosti in zaposlene za zbiranje informacij o ranljivostih in kibernetskih grožnjah, incidentih, povezanih z IKT, zlasti kibernetskih napadih, in analizo njihovih verjetnih vplivov na digitalno operativno odpornost finančnih subjektov.

2. Finančni subjekti vzpostavijo preglede po incidentih, povezanih z IKT, ki se opravijo po tem, ko večji incidenti, povezani z IKT, povzročijo motnje v njihovih osnovnih dejavnostih, in s katerimi analizirajo vzroke motnje in identificirajo potrebne izboljšave v delovanju IKT ali politiki neprekinjenega poslovanja na področju IKT iz člena 11.

Finančni subjekti, ki niso mikropodjetja, pristojnim organom na zahtevo sporočijo spremembe, ki so bile uvedene po pregledih po incidentih, povezanih z IKT, iz prvega pododstavka.

Pri pregledih po incidentih, povezanih z IKT, iz prvega pododstavka se ugotovi, ali so bili upoštevani ustaljeni postopki in ali so bili izvedeni ukrepi učinkoviti, vključno v zvezi z naslednjim:

(a) hitrostjo pri odzivanju na varnostna opozorila ter določanju učinka incidentov, povezanih z IKT, in njihove resnosti;

(b) kakovostjo in hitrostjo izvedbe forenzične analize, kadar je to ustrezno;

(c) učinkovitostjo prenosa incidenta na višjo raven v finančnem subjektu;

(d) učinkovitostjo notranje in zunanje komunikacije.

3. Spoznanja, pridobljena pri testiranju digitalne operativne odpornosti, izvedenem v skladu s členoma 26 in 27, in pri resničnih incidentih, povezanih z IKT, zlasti kibernetskih napadih, se skupaj z izzivi, ki se pojavljajo pri aktivaciji načrtov neprekinjenega poslovanja na področju IKT ter načrtov odzivanja in okrevanja IKT, ter ustreznimi informacijami, izmenjanimi z nasprotnimi strankami in ocenjenimi med nadzornimi pregledi, stalno vključujejo v postopek ocene tveganj na področju IKT. Te ugotovitve tvorijo podlago za ustrezne preglede zadevnih komponent okvira za obvladovanje tveganj na področju IKT iz člena 6(1).

4. Finančni subjekti spremljajo učinkovitost izvajanja svoje strategije za digitalno odpornost iz člena 6(8). Popišejo razvoj tveganj na področju IKT skozi čas, analizirajo pogostost, vrste, obseg in razvoj incidentov, povezanih z IKT, zlasti kibernetskih napadov in njihovih vzorcev, da bi razumeli stopnjo izpostavljenosti tveganju na področju IKT, zlasti v povezavi s kritičnimi ali pomembnimi funkcijami, ter okrepili kibernetsko zrelost in pripravljenost finančnega subjekta.

5. Višji uslužbenci na področju IKT vsaj enkrat letno poročajo upravljalnemu organu o ugotovitvah iz odstavka 3 in podajo priporočila.

6. Finančni subjekti oblikujejo programe ozaveščanja o varnosti na področju IKT in usposabljanje na področju digitalne operativne odpornosti kot obvezne module v svojih shemah za usposabljanje osebja. Ti programi in usposabljanje se uporabljajo za vse zaposlene in za višje vodstvene delavce, njihova raven zahtevnosti pa mora biti sorazmerna s pristojnostmi v okviru njihovih funkcij. Finančni subjekti v svoje ustrezne sheme usposabljanja v skladu s členom 30(2), točka (i), po potrebi vključijo tudi tretje ponudnike storitev IKT.

7. Finančni subjekti, ki niso mikropodjetja, stalno spremljajo ustrezen tehnološki razvoj, tudi zato, da bi razumeli možne vplive uvajanja takih novih tehnologij na zahteve za varnost IKT in digitalno operativno odpornost. Seznanjeni morajo biti z najnovejšimi postopki obvladovanja tveganj na področju IKT, tako da lahko učinkovito preprečujejo sedanje ali nove oblike kibernetskih napadov.

Člen 14

Obveščanje

1. V sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) finančni subjekti pripravijo načrte obveščanja o kriznih razmerah, ki omogočajo odgovorno razkritje vsaj večjih incidentov ali ranljivosti, povezanih z IKT, strankam in partnerjem ter javnosti, kot je ustrezno.

2. V sklopu okvira za obvladovanje tveganj na področju IKT finančni subjekti izvajajo politike obveščanja za notranje zaposlene in zunanje deležnike. Pri politikah obveščanja za zaposlene je treba razlikovati med zaposlenimi, ki sodelujejo pri obvladovanju tveganj na področju IKT, zlasti tistimi, ki so odgovorni za odzivanje in okrevanje, ter zaposlenimi, ki jih je treba le obvestiti.

3. Vsaj ena oseba pri finančnem subjektu je odgovorna za izvajanje strategije obveščanja za incidente, povezane z IKT, in zaseda funkcijo pristojnega za stike z javnostjo in mediji v ta namen.

Člen 15

Nadaljnje usklajevanje orodij, metod, postopkov in politik za obvladovanje tveganj na področju IKT

Evropski nadzorni organi prek Skupnega odbora in v posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA) pripravijo skupne osnutke regulativnih tehničnih standardov za:

(a) podrobno določitev nadaljnjih elementov, ki jih je treba vključiti v varnostne politike, postopke, protokole in orodja IKT iz člena 9(2), da bi se zagotovila varnost omrežij, omogočili ustrezni zaščitni ukrepi pred vdori in zlorabo podatkov, ohranila razpoložljivost, avtentičnost, celovitost in zaupnost podatkov, vključno z uporabo kriptografskih tehnik, ter zagotovil natančen in hiter prenos podatkov brez večjih motenj in nepotrebnih zamud;

(b) razvoj nadaljnjih komponent za nadzor pravic upravljanja dostopa iz člena 9(4), točka (c), in s tem povezane kadrovske politike, ki določajo pravice dostopa, postopke za podeljevanje in odvzem pravic ter spremljanje neobičajnega ravnanja v zvezi s tveganjem na področju IKT z ustreznimi kazalniki, tudi za vzorce uporabe omrežja, ure, dejavnost IT in neznane naprave;

(c) nadaljnji razvoj mehanizmov iz člena 10(1), ki omogočajo takojšnje odkrivanje neobičajnega ravnanja, in meril iz člena 10(2), ki sprožijo postopke odkrivanja incidentov, povezanih z IKT, in odzivanja nanje;

(d) nadaljnjo opredelitev komponent politike neprekinjenega poslovanja na področju IKT iz člena 11(1);

(e) nadaljnjo opredelitev testiranja načrtov neprekinjenega poslovanja na področju IKT iz člena 11(6), da se zagotovi, da se pri takem testiranju ustrezno upoštevajo scenariji, v katerih kakovost zagotavljanja kritične ali pomembne funkcije pade na nesprejemljivo raven ali povsem odpove, in ustrezno upošteva potencialni vpliv plačilne nesposobnosti ali drugega prenehanja delovanja katerega koli zadevnega tretjega ponudnika storitev IKT in, kadar je to ustrezno, politična tveganja v jurisdikcijah teh ponudnikov;

(f) nadaljnjo opredelitev komponent načrtov odzivanja in okrevanja na področju IKT iz člena 11(3);

(g) nadaljnjo opredelitev vsebine in oblike poročila o pregledu okvira za obvladovanje tveganj na področju IKT iz člena 6(5).

Evropski nadzorni organi pri pripravi teh osnutkov regulativnih tehničnih standardov upoštevajo velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja, pri čemer ustrezno upoštevajo vse specifične značilnosti, ki izhajajo iz posebne narave dejavnosti v različnih sektorjih finančnih storitev.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. januarja 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega odstavka v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 16

Poenostavljen okvir za obvladovanje tveganj na področju IKT

1. Členi 5 do 15 te uredbe se ne uporabljajo za mala in nepovezana investicijska podjetja ter plačilne institucije, izvzete na podlagi Direktive (EU) 2015/2366, institucije, izvzete na podlagi Direktive 2013/36/EU, v zvezi s katerimi so se države članice odločile, da ne bodo uporabile možnosti iz člena 2(4) te uredbe, institucije za izdajo elektronskega denarja, izvzete na podlagi Direktive 2009/110/ES, ter male institucije za poklicno pokojninsko zavarovanje.

Brez poseganja v prvi pododstavek morajo finančni subjekti iz prvega pododstavka:

(a) vzpostaviti in vzdrževati zanesljiv in dokumentiran okvir za obvladovanje tveganj na področju IKT, v katerem so podrobno določeni mehanizmi in ukrepi za hitro, učinkovito in celovito obvladovanje tveganj na področju IKT, vključno z zaščito ustreznih fizičnih komponent in infrastrukture;

(b) stalno preverjati varnost in delovanje vseh sistemov IKT;

(c) čim bolj zmanjšati vpliv tveganja na področju IKT z uporabo zanesljivih, odpornih in posodobljenih sistemov, protokolov in orodij IKT, ki so primerni za podporo izvajanju njihovih dejavnosti in opravljanju storitev ter ustrezno varujejo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov v omrežju in informacijskih sistemih;

(d) omogočiti hitro identifikacijo in odkrivanje virov tveganja in nepravilnosti na področju IKT v omrežnih in informacijskih sistemih ter hitro obravnavo incidentov, povezanih z IKT;

(e) identificirati ključne odvisnosti od tretjih ponudnikov storitev IKT;

(f) zagotavljati neprekinjenost kritičnih ali pomembnih funkcij z načrti neprekinjenega poslovanja ter ukrepi za odzivanje in okrevanje, ki vključujejo vsaj ukrepe za varnostno kopiranje in obnovitev;

(g) redno testirati načrte in ukrepe iz točke (f) ter učinkovitost preverjanj, izvedenih v skladu s točkama (a) in (c);

(h) po potrebi ustrezne operativne sklepe, pripravljene na podlagi testov iz točke (g) in analize po incidentu, vključiti v postopek ocene tveganja na področju IKT ter v skladu s potrebami in profilom tveganja na področju IKT razvijati programe za usposabljanje in ozaveščanje osebja in vodstva glede varnosti IKT in digitalne operativne odpornosti.

2. Okvir za obvladovanje tveganj na področju IKT iz odstavka 1, drugi pododstavek, točka (a), se dokumentira ter pregleduje, redno in ob pojavu večjih incidentov, povezanih z IKT, v skladu z nadzorniškimi navodili. Nenehno se izboljšuje na podlagi izkušenj, pridobljenih pri izvajanju in spremljanju. Poročilo o pregledu okvira za obvladovanje tveganj na področju IKT se posreduje pristojnemu organu na njegovo zahtevo.

3. Evropski nadzorni organi prek Skupnega odbora in v posvetovanju z ENISA pripravijo skupne osnutke regulativnih tehničnih standardov, da:

(a) nadalje opredelijo elemente, ki jih je treba vključiti v okvir za obvladovanje tveganj na področju IKT iz odstavka 1, drugi pododstavek, točka (a);

(b) nadalje opredelijo elemente v zvezi s sistemi, protokoli in orodji za zmanjšanje vpliva tveganj na področju IKT iz odstavka 1, drugi pododstavek, točka (c), da se zagotovi varnost omrežij, omogočijo ustrezni zaščitni ukrepi pred vdori in zlorabo podatkov ter ohranijo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov;

(c) nadalje opredelijo komponente načrtov neprekinjenega poslovanja na področju IKT iz odstavka 1, drugi pododstavek, točka (f);

(d) nadalje opredelijo pravila o testiranju načrtov neprekinjenega poslovanja in zagotavljanje učinkovitosti kontrol iz odstavka 1, drugi pododstavek, točka (g), ter zagotovijo, da se pri takem testiranju ustrezno upoštevajo scenariji, v katerih kakovost zagotavljanja kritične ali pomembne funkcije pade na nesprejemljivo raven ali povsem odpove;

(e) nadalje opredelijo vsebino in obliko poročila o pregledu okvira za obvladovanje tveganj na področju IKT iz odstavka 2.

Evropski nadzorni organi pri oblikovanju navedenih osnutkov regulativnih tehničnih standardov upoštevajo velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in operacij.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. januarja 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

POGLAVJE III

Obvladovanje in razvrščanje incidentov, povezanih z IKT, ter poročanje o njih

Člen 17

Postopek obvladovanja incidentov, povezanih z IKT

1. Finančni subjekti opredelijo, vzpostavijo in izvajajo postopek obvladovanja incidentov, povezanih z IKT, za odkrivanje in obvladovanje incidentov, povezanih z IKT, ter obveščanje o njih.

2. Finančni subjekti evidentirajo vse incidente, povezane z IKT, in pomembne kibernetske grožnje. Finančni subjekti vzpostavijo ustrezne postopke in procese za zagotovitev doslednega in celovitega spremljanja, obravnavanja in nadaljnjega spremljanja incidentov, povezanih z IKT, da se zagotovi identificiranje, dokumentiranje in obravnavanje temeljnih vzrokov ter s tem prepreči pojavljanje tovrstnih incidentov.

3. V postopku obvladovanja incidentov, povezanih z IKT, iz odstavka 1 se:

(a) vzpostavijo kazalniki za zgodnje opozarjanje;

(b) vzpostavijo postopki za identifikacijo, sledenje, evidentiranje, kategoriziranje in razvrščanje incidentov, povezanih z IKT, glede na njihovo prioriteto in resnost ter glede na kritičnost prizadetih storitev v skladu z merili, določenimi v členu 18(1);

(c) dodelijo vloge in odgovornosti, ki jih je treba aktivirati za različne vrste in scenarije incidentov, povezanih z IKT;

(d) določijo načrti za obveščanje zaposlenih, zunanjih deležnikov in medijev v skladu s členom 14 ter za obveščanje strank, za postopke notranjega prenosa na višjo raven, vključno s pritožbami strank v zvezi z IKT, ter za zagotavljanje informacij finančnim subjektom, ki delujejo kot partnerji, kot je ustrezno;

(e) zagotovi, da se vsaj o večjih incidentih, povezanih z IKT, poroča ustreznim višjim vodstvenim delavcem, in o njih obvesti upravljalni organ, pri čemer se pojasnijo vpliv, odziv in dodatne kontrole, ki jih je treba vzpostaviti zaradi tovrstnih incidentov, povezanih z IKT;

(f) vzpostavijo postopki odzivanja na incidente, povezane z IKT, za zmanjšanje njihovih učinkov in zagotovitev, da začnejo storitve delovati pravočasno in varno.

Člen 18

Razvrščanje incidentov, povezanih z IKT, in kibernetskih groženj

1. Finančni subjekti razvrstijo incidente, povezane z IKT, in določijo njihov učinek na podlagi naslednjih meril:

(a) število uporabnikov in/ali pomembnost strank ali finančnih partnerjev, ki jih je prizadela motnja zaradi incidenta, povezanega z IKT, in po potrebi količino oziroma število transakcij, na katere so ti incidenti vplivali, ter podatek, ali je incident, povezan z IKT, vplival na njihov ugled;

(b) trajanje incidenta, povezanega z IKT, vključno z nedelovanjem storitve;

(c) geografska razpršenost območij, ki jih je prizadel incident, povezan z IKT, zlasti če prizadene več kot dve državi članici;

(d) izgube podatkov, ki jih povzroči incident, povezan z IKT, v smislu razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti podatkov;

(e) kritičnost prizadetih storitev, vključno s transakcijami in poslovanjem finančnega subjekta;

(f) gospodarski učinek – zlasti neposredni in posredni stroški in izgube – incidenta, povezanega z IKT, v absolutnem in relativnem smislu.

2. Finančni subjekti kibernetske grožnje razvrstijo kot pomembne na podlagi kritičnosti storitev, pri katerih obstaja tveganje, vključno s transakcijami in operacijami finančnega subjekta, številom in/ali pomembnostjo ciljnih strank ali finančnih partnerjev ter geografsko razpršenostjo ogroženih območij.

3. Evropski nadzorni organi prek Skupnega odbora in v posvetovanju z ECB in ENISA pripravijo skupne osnutke regulativnih tehničnih standardov, v katerih se podrobneje določijo:

(a) merila iz odstavka 1, vključno s pragovi pomembnosti za določanje večjih incidentov, povezanih z IKT, oziroma večjih operativnih ali varnostnih incidentov, povezanih s plačili, za katere velja obveznost poročanja iz člena 19(1);

(b) merila, ki jih pristojni organi uporabijo za oceno pomena večjih incidentov, povezanih z IKT, oziroma večjih operativnih ali varnostnih incidentov, povezanih s plačili, za ustrezne pristojne organe v drugih državah članicah, in podrobnosti poročil o večjih incidentih, povezanih z IKT, oziroma večjih operativnih ali varnostnih incidentih, povezanih s plačili, ki jih je treba deliti z drugimi pristojnimi organi v skladu s členom 19(6) in (7);

(c) merila iz odstavka 2 tega člena, vključno z visokimi pragovi pomembnosti za določanje pomembnih kibernetskih groženj.

4. Evropski nadzorni organi pri pripravi skupnih osnutkov regulativnih tehničnih standardov iz odstavka 3 tega člena upoštevajo merila, določena v členu 4(2), ter mednarodne standarde, smernice in specifikacije, ki jih je razvila in objavila ENISA, vključno s specifikacijami za druge gospodarske sektorje, kadar je to ustrezno. Evropski nadzorni organi za namene uporabe meril, določenih v členu 4(2), ustrezno upoštevajo, da morajo mikropodjetja ter mala in srednja podjetja mobilizirati zadostna sredstva in zmožnosti za zagotovitev hitrega obvladovanja incidentov, povezanih z IKT.

Evropski nadzorni organi te skupne osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. januarja 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz odstavka 3 v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 19

Poročanje o večjih incidentih, povezanih z IKT, in prostovoljno obveščanje o pomembnih kibernetskih grožnjah

1. Finančni subjekti o večjih incidentih, povezanih z IKT, poročajo ustreznemu pristojnemu organu iz člena 46 v rokih v skladu z odstavkom 4 tega člena.

Kadar finančni subjekt nadzira več kot en nacionalni pristojni organ iz člena 46, države članice imenujejo en sam pristojni organ kot ustrezni pristojni organ, odgovoren za izvajanje funkcij in dolžnosti iz tega člena.

Kreditne institucije, razvrščene kot pomembne v skladu s členom 6(4) Uredbe (EU) št. 1024/2013, poročajo o večjih incidentih, povezanih z IKT, ustreznemu nacionalnemu pristojnemu organu, imenovanemu v skladu s členom 4 Direktive 2013/36/EU, ki to poročilo nemudoma posreduje ECB.

Za namene prvega pododstavka finančni subjekti po zbiranju in analizi vseh ustreznih informacij v skladu s predlogami iz člena 20 pripravijo začetno uradno obvestilo in poročila iz odstavka 4 tega člena in jih posredujejo pristojnemu organu. Če začetnega uradnega obvestila zaradi tehničnih razlogov ni mogoče predložiti v skladu s predlogo, finančni subjekti pristojni organ o njem uradno obvestijo na drug način.

Začetno uradno obvestilo in poročila iz odstavka 4 vključujejo vse informacije, ki so potrebne, da pristojni organ ugotovi pomen večjega incidenta, povezanega z IKT, in oceni možne čezmejne učinke.

Brez poseganja v poročanje finančnega subjekta ustreznemu pristojnemu organu na podlagi prvega pododstavka lahko države članice dodatno določijo, da nekateri ali vsi finančni subjekti začetno uradno obvestilo in vsako poročilo iz odstavka 4 tega člena v skladu s predlogo iz člena 20 predložijo tudi pristojnim organom ali skupinam za odzivanje na incidente na področju računalniške varnosti (CSIRT), imenovanim ali vzpostavljenim v skladu z Direktivo (EU) 2022/2555.

2. Finančni subjekti lahko o pomembnih kibernetskih grožnjah prostovoljno uradno obvestijo ustrezni pristojni organ, če menijo, da je grožnja relevantna za finančni sistem, uporabnike storitev ali stranke. Ustrezni pristojni organ lahko te informacije posreduje drugim ustreznim organom iz odstavka 6.

Kreditne institucije, razvrščene kot pomembne v skladu s členom 6(4) Uredbe (EU) št. 1024/2013, lahko o pomembnih kibernetskih grožnjah prostovoljno uradno obvestijo ustrezni nacionalni pristojni organ, imenovan v skladu s členom 4 Direktive 2013/36/EU, ki to obvestilo nemudoma posreduje ECB.

Države članice lahko določijo, da lahko finančni subjekti, ki prostovoljno pošljejo uradno obvestilo v skladu s prvim pododstavkom, to obvestilo posredujejo tudi skupinam CSIRT, imenovanim ali vzpostavljenim v skladu z Direktivo (EU) 2022/2555.

3. V primeru večjega incidenta, povezanega z IKT, ki vpliva na finančne interese strank, finančni subjekti takoj, ko izvedo za incident, brez nepotrebnega odlašanja obvestijo svoje stranke o njem in o ukrepih, ki so bili sprejeti za zmanjšanje njegovih škodljivih učinkov.

V primeru pomembne kibernetske grožnje finančni subjekti svoje stranke, ki bi lahko bile prizadete, po potrebi obvestijo o vseh ustreznih zaščitnih ukrepih, ki bi jih te lahko sprejele.

4. Finančni subjekti v rokih, ki se določijo v skladu s členom 20, prvi odstavek, točka (a), točka (ii), ustreznemu pristojnemu organu predložijo naslednje:

(a) začetno uradno obvestilo;

(b) vmesno poročilo po začetnem uradnem obvestilu iz točke (a), takoj ko se status prvotnega incidenta znatno spremeni ali ko se obravnava incidenta prilagodi glede na nove informacije, ki so na voljo, ki mu, kot je ustrezno, sledijo ustrezna posodobljena uradna obvestila vsakič, ko je na voljo ustrezna posodobitev statusa, in na posebno zahtevo pristojnega organa;

(c) končno poročilo, ko je končana analiza osnovnega vzroka, ne glede na to, ali so bili ukrepi za ublažitev že izvedeni, in ko so na voljo podatki o dejanskem učinku, ki nadomeščajo ocene.

5. Finančni subjekti lahko v skladu s sektorskim pravom Unije in nacionalnim sektorskim pravom obveznosti poročanja iz tega člena oddajo v zunanje izvajanje tretjemu ponudniku storitev. V primerih tovrstnega zunanjega izvajanja finančni subjekt ostane v celoti odgovoren za izpolnjevanje zahtev glede poročanja o incidentih.

6. Pristojni organ po prejemu začetnega uradnega obvestila in vsakega poročila iz odstavka 4 pravočasno zagotovi podrobnosti o večjem incidentu, povezanem z IKT, naslednjim prejemnikom, in sicer na podlagi njihovih pristojnosti, kot je ustrezno:

(a) EBA, ESMA ali EIOPA;

(b) ECB, za finančne subjekte iz člena 2(1), točke (a), (b) in (d);

(c) pristojnim organom, enotnim kontaktnim točkam oziroma skupinam CSIRT, imenovanim ali vzpostavljenim v skladu z Direktivo (EU) 2022/2555;

(d) organom za reševanje iz člena 3 Direktive 2014/59/EU in enotnemu odboru za reševanje, kar zadeva subjekte iz člena 7(2) Uredbe (EU) št. 806/2014 Evropskega parlamenta in Sveta ([37]) ter subjekte in skupine iz člena 7(4)(b) in (5) Uredbe (EU) št. 806/2014, če se te podrobnosti nanašajo na incidente, ki predstavljajo tveganje za zagotavljanje kritičnih funkcij v smislu člena 2(1), točka 35, Direktive 2014/59/EU, in

(e) drugim ustreznim javnim organom v skladu z nacionalnim pravom.

7. EBA, ESMA ali EIOPA in ECB po prejemu informacij v skladu z odstavkom 6 v posvetovanju z ENISA ter v sodelovanju z ustreznim pristojnim organom ocenijo, ali večji incident, povezan z IKT, zadeva pristojne organe v drugih državah članicah. EBA, ESMA ali EIOPA po tej oceni o tem čim prej uradno obvestijo ustrezne pristojne organe v drugih državah članicah. ECB člane Evropskega sistema centralnih bank obvesti o zadevah, pomembnih za plačilni sistem. Pristojni organi na podlagi obvestila, kadar je ustrezno, sprejmejo vse potrebne ukrepe za zagotovitev takojšnje stabilnosti finančnega sistema.

([37]) Uredba (EU) št. 806/2014 Evropskega parlamenta in Sveta z dne 15. julija 2014 o določitvi enotnih pravil in enotnega postopka za reševanje kreditnih institucij in določenih investicijskih podjetij v okviru enotnega mehanizma za reševanje in enotnega sklada za reševanje ter o spremembi Uredbe (EU) št. 1093/2010 (UL L 225, 30.7.2014, str. 1).

8. Uradno obvestilo, ki ga ESMA pošlje na podlagi odstavka 7 tega člena, ne posega v odgovornost pristojnega organa, da nemudoma posreduje podrobnosti o večjem incidentu, povezanem z IKT, ustreznemu organu v državi članici gostiteljici, kadar centralna depotna družba opravlja pomembno čezmejno dejavnost v državi članici gostiteljici, kadar bo večji incident, povezan z IKT, verjetno imel resne posledice za finančne trge države članice gostiteljice ter kadar med pristojnimi organi obstajajo dogovori o sodelovanju v zvezi z nadzorom finančnih subjektov.

Člen 20

Harmonizacija vsebine in predlog za poročanje

Evropski nadzorni organi prek Skupnega odbora in v posvetovanju z ENISA in ECB razvijejo:

(a) skupne osnutke regulativnih tehničnih standardov, da:

(i) določijo vsebino poročil o večjih incidentih, povezanih z IKT, da se upoštevajo merila iz člena 18(1) in vključijo dodatni elementi, kot so podrobnosti, ki omogočajo, da se ugotovi relevantnost poročanja za druge države članice in ali gre za večji operativni ali varnostni incident, povezan s plačilom, ali ne;

(ii) določijo roke za začetno obvestilo in za vsako poročilo iz člena 19(4);

(iii) določijo vsebino obvestila o pomembnih kibernetskih grožnjah.

Evropski nadzorni organi pri oblikovanju navedenih osnutkov regulativnih tehničnih standardov upoštevajo velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja, zlasti, da se za namene tega odstavka, točka (a), točka (ii), zagotovi, da lahko različni roki po potrebi odražajo posebnosti finančnih sektorjev, brez poseganja v ohranjanje doslednega pristopa k poročanju o incidentih, povezanih z IKT, v skladu s to uredbo in Direktivo (EU) 2022/2555. Evropski nadzorni organi po potrebi utemeljijo odstopanje od pristopov, sprejetih v okviru navedene direktive;

(b) skupne osnutke izvedbenih tehničnih standardov, da vzpostavijo standardne obrazce, predloge in postopke, v okviru katerih finančni subjekti poročajo o večjem incidentu, povezanem z IKT, in uradno obveščajo o pomembni kibernetski grožnji.

Evropski nadzorni organi skupne osnutke regulativnih tehničnih standardov iz prvega odstavka, točka (a), in skupne osnutke izvedbenih tehničnih standardov iz prvega odstavka, točka (b), predložijo Komisiji do 17. julija 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem skupnih regulativnih tehničnih standardov iz prvega odstavka, točka (a), v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Na Komisijo se prenese pooblastilo za sprejetje skupnih izvedbenih tehničnih standardov iz prvega odstavka, točka (b), v skladu s členom 15 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 21

Centralizacija poročanja o večjih incidentih, povezanih z IKT

1. Evropski nadzorni organi prek Skupnega odbora in v posvetovanju z ECB in ENISA pripravijo skupno poročilo, v katerem ocenijo izvedljivost nadaljnje centralizacije poročanja o incidentih z vzpostavitvijo enotnega vozlišča EU, kjer lahko finančni subjekti poročajo o večjih incidentih, povezanih z IKT. V skupnem poročilu se preuči, kako olajšati pretok poročanja o incidentih, povezanih z IKT, znižati s tem povezane stroške in podpirati tematske analize za povečanje konvergence nadzora.

2. Skupno poročilo iz odstavka 1 vsebuje vsaj naslednje elemente:

(a) pogoje za vzpostavitev enotnega vozlišča EU;

(b) koristi, omejitve in tveganja, vključno s tveganji, povezanimi z visoko koncentracijo občutljivih informacij;

(c) potrebne zmožnosti za zagotovitev interoperabilnosti glede na druge zadevne sheme poročanja;

(d) elemente operativnega upravljanja;

(e) pogoje članstva;

(f) tehnične ureditve za dostop finančnih subjektov in nacionalnih pristojnih organov do enotnega vozlišča EU;

(g) predhodno oceno finančnih stroškov, ki nastanejo zaradi vzpostavitve operativne platforme za podporo enotnega vozlišču EU, vključno z zahtevanim strokovnim znanjem.

3. Evropski nadzorni organi poročilo iz odstavka 1 predložijo Evropskemu parlamentu, Svetu in Komisiji do 17. januarja 2025.

Člen 22

Povratne informacije nadzornih organov

1. Brez poseganja v tehnične prispevke, nasvete ali popravne ukrepe ter nadaljnje ukrepe, ki jih lahko po potrebi v skladu z nacionalnim pravom skupine CSIRT zagotovijo na podlagi Direktive (EU) 2022/2555, pristojni organ po prejemu začetnega uradnega obvestila in vsakega poročila iz člena 19(4) potrdi prejem ter lahko, kadar je to mogoče, finančnemu subjektu pravočasno zagotovi ustrezne in sorazmerne povratne informacije ali smernice na visoki ravni, zlasti z omogočanjem dostopa do relevantnih anonimiziranih informacij in podatkov o podobnih grožnjah, ter lahko razpravlja o popravnih ukrepih, izvedenih na ravni finančnega subjekta, in načinih za zmanjšanje in ublažitev škodljivih vplivov v finančnem sektorju. Brez poseganja v prejete povratne informacije nadzornih organov so finančni subjekti še naprej v celoti odgovorni za obravnavo incidentov, povezanih z IKT, o katerih se poroča na podlagi člena 19(1), in za njihove posledice.

2. Evropski nadzorni organi prek Skupnega odbora na anonimni podlagi in združeno enkrat letno poročajo o večjih incidentih, povezanih z IKT, katerih podrobnosti zagotovijo pristojni organi v skladu s členom 19(6), pri čemer navedejo vsaj število večjih incidentov, povezanih z IKT, njihovo naravo, njihov učinek na poslovanje finančnih subjektov ali strank, izvedene popravne ukrepe in nastale stroške.

Evropski nadzorni organi izdajo opozorila in pripravijo statistične podatke na visoki ravni v podporo ocenam groženj in ranljivosti na področju IKT.

Člen 23

Operativni ali varnostni incidenti, povezani s plačili, ki zadevajo kreditne institucije, plačilne institucije, ponudnike storitev zagotavljanja informacij o računih ter institucije za izdajo elektronskega denarja

Zahteve iz tega poglavja se uporabljajo tudi za operativne ali varnostne incidente, povezane s plačili, in večje tovrstne incidente, kadar zadevajo kreditne institucije, plačilne institucije, ponudnike storitev zagotavljanja informacij o računih ter institucije za izdajo elektronskega denarja.

POGLAVJE IV

Testiranje digitalne operativne odpornosti

Člen 24

Splošne zahteve za izvajanje testiranja digitalne operativne odpornosti

1. Finančni subjekti, ki niso mikropodjetja, za namene ocenjevanja pripravljenosti na obvladovanje incidentov, povezanih z IKT, identificiranja slabosti, pomanjkljivosti in vrzeli v digitalni operativni odpornosti in takojšnjega izvajanja popravnih ukrepov ob upoštevanju meril iz člena 4(2) vzpostavijo, vzdržujejo in pregledujejo trden in celovit program za testiranje digitalne operativne odpornosti v sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6.

2. V program za testiranje digitalne operativne odpornosti se vključi vrsta ocen, testov, metodologij, praks in orodij, ki se uporabljajo v skladu s členoma 25 in 26.

3. Finančni subjekti, ki niso mikropodjetja, pri izvajanju programa za testiranje digitalne operativne odpornosti iz odstavka 1 tega člena sledijo pristopu, ki temelji na tveganju, pri čemer upoštevajo merila, določena v členu 4(2), tako da ustrezno pozornost namenijo spreminjajoči se krajini tveganj na področju IKT, morebitnim posebnim tveganjem, ki jim je zadevni finančni subjekt izpostavljen ali bi lahko bil izpostavljen, kritičnosti informacijskih sredstev in storitev, ki se opravljajo, ter vsem drugim dejavnikom, ki se jim zdijo ustrezni.

4. Finančni subjekti, ki niso mikropodjetja, zagotovijo, da teste izvajajo notranje ali zunanje neodvisne strani. Kadar teste izvajajo notranji preizkuševalci, finančni subjekti temu namenijo zadostna sredstva in zagotovijo, da se v fazi zasnove in izvedbe testa preprečijo nasprotja interesov.

5. Finančni subjekti, ki niso mikropodjetja, vzpostavijo postopke in politike za prednostno obravnavo, razvrstitev in odpravo vseh težav, ki so se pokazale med izvajanjem testov, ter vzpostavijo notranje metodologije za validacijo, da ugotovijo, ali so v celoti obravnavane vse identificirane slabosti, pomanjkljivosti ali vrzeli.

6. Finančni subjekti, ki niso mikropodjetja, vsaj enkrat letno zagotovijo, da se ustrezno testirajo vsi sistemi in aplikacije IKT, ki podpirajo kritične ali pomembne funkcije.

Člen 25

Testiranje sistemov in orodij IKT

1. Program za testiranje digitalne operativne odpornosti iz člena 24 zagotavlja – v skladu z merili, določenimi v členu 4(2), – izvajanje ustreznih testov, kot so ocene in pregledi ranljivosti, analize odprtokodne programske opreme, ocene varnosti omrežja, analize vrzeli, pregledi fizične varnosti, vprašalniki in rešitve za preiskovanje programske opreme, pregledi izvorne kode, kadar je to mogoče, testiranja na podlagi scenarijev, testi združljivosti, testi učinkovitosti, celovita testiranja in penetracijsko testiranje.

2. Centralne depotne družbe in centralne nasprotne stranke izvedejo ocene ranljivosti pred kakršno koli uvedbo ali prerazporeditvijo novih ali obstoječih aplikacij in infrastruturnih komponent ter storitev IKT, ki podpirajo kritične ali pomembne funkcije finančnega subjekta.

3. Mikropodjetja opravijo teste iz odstavka 1 tako, da združijo pristop, ki temelji na tveganju, s strateškim načrtovanjem testiranja IKT, pri čemer ustrezno upoštevajo potrebo po ohranjanju uravnoteženega pristopa med obsegom virov in časom, ki se nameni testu IKT iz tega člena, na eni strani ter nujnostjo, vrsto tveganja, kritičnostjo informacijskih sredstev in opravljenih storitev ter kakršnimi koli drugimi ustreznimi dejavniki, vključno z zmožnostjo finančnega subjekta, da premišljeno tvega, na drugi strani.

Člen 26

Napredno testiranje orodij, sistemov in postopkov IKT na podlagi penetracijskega testiranja na podlagi analize groženj

1. Finančni subjekti, ki niso subjekti iz člena 16(1), prvi pododstavek, in niso mikropodjetja ter so opredeljeni v skladu z odstavkom 8, tretji pododstavek, tega člena vsaj vsaka tri leta izvedejo napredno penetracijsko testiranje na podlagi analize groženj. Na podlagi profila tveganja finančnega subjekta in ob upoštevanju operativnih okoliščin lahko pristojni organ po potrebi od finančnega subjekta zahteva, da to stori manj ali bolj pogosto.

2. Vsak penetracijski test na podlagi analize groženj zajema nekatere ali vse kritične ali pomembne funkcije finančnega subjekta ter se izvaja na aktivnih produkcijskih sistemih, ki podpirajo take funkcije.

Finančni subjekti identificirajo vse ustrezne osnovne sisteme, postopke in tehnologije IKT, ki podpirajo kritične ali pomembne funkcije ter storitve IKT, vključno s tistimi, ki podpirajo kritične ali pomembne funkcije, ki so oddane v zunanje izvajanje ali pogodbeno izvajanje tretjim ponudnikom storitev IKT.

Finančni subjekti ocenijo, katere kritične ali pomembne funkcije morajo biti zajete v penetracijsko testiranje na podlagi analize groženj. Rezultat te ocene določi natančen obseg penetracijskega testiranja na podlagi analize groženj, potrdijo pa ga pristojni organi.

3. Kadar so tretji ponudniki storitev IKT vključeni v obseg penetracijskega testiranja na podlagi analize groženj, finančni subjekt sprejme potrebne in zaščitne ukrepe, da zagotovi sodelovanje teh tretjih ponudnikov storitev IKT pri penetracijskem testiranju na podlagi analize groženj, ter je ves čas v celoti odgovoren za izpolnjevanje obveznosti iz te uredbe.

4. Brez poseganja v odstavek 2, prvi in drugi pododstavek, se lahko finančni subjekt in tretji ponudnik storitev IKT, kadar se razumno pričakuje, da bo sodelovanje tretjega ponudnika storitev IKT pri penetracijskem testiranju na podlagi analize groženj iz odstavka 3 škodljivo vplivalo na kakovost ali varnost storitev, ki jih tretji ponudnik storitev IKT zagotavlja strankam, ki so subjekti, ki ne spadajo na področje uporabe te uredbe, ali na zaupnost podatkov, povezanih s takimi storitvami, pisno dogovorita, da tretji ponudnik storitev IKT sklene pogodbene dogovore neposredno z zunanjim preizkuševalcem, z namenom da se pod vodstvom enega imenovanega finančnega subjekta izvede skupno penetracijsko testiranje na podlagi analize groženj, ki vključuje več finančnih subjektov (skupno testiranje), za katere tretji ponudnik storitev IKT opravlja storitve IKT.

To skupno testiranje zajema ustrezen nabor storitev IKT, ki podpirajo kritične ali pomembne funkcije, ki jih finančni subjekti v skladu s pogodbo zagotavljajo zadevnim tretjim ponudnikom storitev IKT. Skupno testiranje se šteje za penetracijsko testiranje na podlagi analize groženj, ki ga izvajajo finančni subjekti, ki sodelujejo pri skupnem testiranju.

Število finančnih subjektov, ki sodelujejo pri skupnem testiranju, se ustrezno prilagodi glede na kompleksnost in vrsto storitev, ki so v to vključene.

5. Finančni subjekti v sodelovanju s tretjimi ponudniki storitev IKT in udeleženimi stranmi, vključno s preizkuševalci, ne pa s pristojnimi organi, uporabljajo učinkovite kontrole za obvladovanje tveganj, da ublažijo tveganja morebitnega vpliva na podatke, škodo na sredstvih in motnje v kritičnih ali pomembnih funkcijah, storitvah ali poslovanju samega finančnega subjekta, njegovih nasprotnih strank ali v finančnem sektorju.

6. Na koncu testiranja, po dogovoru glede poročil in sanacijskih načrtov, finančni subjekt in po potrebi zunanji preizkuševalci organu, imenovanemu v skladu z odstavkom 9 ali 10, predložijo povzetek relevantnih ugotovitev, sanacijske načrte in dokumentacijo, ki dokazuje, da je bilo penetracijsko testiranje na podlagi analize groženj izvedeno v skladu z zahtevami.

7. Organi finančnim subjektom izdajo potrdilo, da je bilo testiranje izvedeno v skladu z zahtevami, kot je razvidno iz dokumentacije, da bi lahko pristojni organi penetracijske teste na podlagi analize groženj vzajemno priznali. Finančni subjekt ustrezni pristojni organ uradno obvesti o potrdilu, povzetku relevantnih ugotovitev in sanacijskih načrtih.

Brez poseganja v takšno potrdilo so finančni subjekti vedno v celoti odgovorni za vpliv testiranj iz odstavka 4.

8. Finančni subjekti za namene izvajanja penetracijskega testiranja na podlagi analize groženj sklenejo pogodbo s preizkuševalci v skladu s členom 27. Ko finančni subjekti uporabljajo notranje preizkuševalce za namene izvajanja penetracijskega testiranja na podlagi analize groženj, sklenejo pogodbo z zunanjim preizkuševalcem za vsak tretji test.

Kreditne institucije, ki so razvrščene kot pomembne v skladu s členom 6(4) Uredbe (EU) št. 1024/2013, uporabljajo zunanje preizkuševalce samo v skladu s členom 27(1), točke (a) do (e).

Pristojni organi finančne subjekte, ki morajo izvesti penetracijsko testiranje na podlagi analize groženj, opredelijo tako, da upoštevajo merila iz člena 4(2), ter na podlagi ocene:

(a) dejavnikov, povezanih z učinki, zlasti v kolikšnem obsegu opravljene storitve in dejavnosti, ki jih izvaja finančni subjekt, vplivajo na finančni sektor;

(b) morebitnih pomislekov glede finančne stabilnosti, vključno s sistemskim značajem finančnega subjekta na ravni Unije ali nacionalni ravni, kot je ustrezno;

(c) posebnega profila tveganja na področju IKT, stopnje zrelosti finančnega subjekta na področju IKT ali značilnosti vključene tehnologije.

9. Države članice lahko imenujejo en sam javni organ v finančnem sektorju, ki bo na nacionalni ravni odgovoren za zadeve, povezane s penetracijskim testiranjem na podlagi analize groženj v finančnem sektorju, in mu v ta namen zaupajo vse pristojnosti in naloge.

10. Brez imenovanja v skladu z odstavkom 9 tega člena in brez poseganja v pooblastilo za opredelitev finančnih subjektov, od katerih se zahteva, da izvedejo penetracijsko testiranje na podlagi analize groženj, lahko pristojni organ prenese izvajanje nekaterih ali vseh nalog iz tega člena in člena 27 na drug nacionalni organ v finančnem sektorju.

11. Evropski nadzorni organi v dogovoru z ECB pripravijo skupne osnutke regulativnih tehničnih standardov v skladu z okvirom TIBER-EU, da bi podrobneje opredelili:

(a) merila, ki veljajo za namene uporabe odstavka 8, drugi pododstavek;

(b) zahteve in standarde, ki urejajo uporabo notranjih preizkuševalcev;

(c) zahteve v zvezi z:

  (i) obsegom penetracijskega testiranja na podlagi analize groženj iz odstavka 2;

  (ii) metodologijo in pristopom testiranja, ki ju je treba upoštevati za vsako posamezno fazo testiranja;

  (iii) rezultati ter zaključno fazo in fazo sanacije;

(d) vrsto sodelovanja nadzornih organov in drugega ustreznega sodelovanja, ki je potrebno za izvedbo penetracijskega testiranja na podlagi analize groženj in njegovo lažje vzajemno priznavanje, kar zadeva finančne subjekte, ki delujejo v več kot eni državi članici, da se omogoči ustrezna raven sodelovanja nadzornih organov in prilagodljivo izvajanje z upoštevanjem posebnosti finančnih podsektorjev ali lokalnih finančnih trgov.

Evropski nadzorni organi pri pripravi teh osnutkov regulativnih tehničnih standardov ustrezno upoštevajo vse specifične značilnosti, ki izhajajo iz posebne narave dejavnosti v različnih sektorjih finančnih storitev.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. julija 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 27

Zahteve za preizkuševalce za izvedbo penetracijskega testiranja na podlagi analize groženj

1. Finančni subjekti za izvedbo penetracijskega testiranja na podlagi analize groženj uporabljajo samo preizkuševalce, ki:

(a) so najprimernejši in uživajo največji ugled;

(b) imajo tehnične in organizacijske zmožnosti ter posebno strokovno znanje na področjih obveščevalnih podatkov o grožnjah, penetracijskega testiranja in testiranja z rdečo ekipo;

(c) so potrjeni s strani akreditacijskega organa v državi članici ali upoštevajo formalne kodekse ravnanja ali etične okvire;

(d) predložijo neodvisno zagotovilo ali revizijsko poročilo v zvezi z dobrim obvladovanjem tveganj, povezanih z izvajanjem penetracijskega testiranja na podlagi analize groženj, vključno z ustrezno zaščito zaupnih podatkov finančnega subjekta in povračilom škode za poslovna tveganja finančnega subjekta;

(e) imajo primerno in polno kritje z ustreznimi zavarovanji poklicne odgovornosti, vključno s kritjem tveganja kršitve in malomarnosti;

2. Kadar uporabijo notranje preizkuševalce, finančni subjekti zagotovijo, da so poleg zahtev iz odstavka 1 izpolnjeni naslednji pogoji:

(a) takšno uporabo odobri ustrezni pristojni organ ali en sam javni organ, imenovan v skladu s členom 26(9) in (10);

(b) ustrezni pristojni organ potrdi, da ima finančni subjekt zadostna sredstva v ta namen, in zagotovi, da se v fazi zasnove in izvedbe testiranja preprečijo nasprotja interesov, ter

(c) ponudnik obveščevalnih podatkov o grožnjah ni del finančnega subjekta.

3. Finančni subjekti zagotovijo, da se v pogodbah, sklenjenih z zunanjimi preizkuševalci, zahteva dobro upravljanje rezultatov penetracijskega testiranja na podlagi analize groženj in da kakršna koli obdelava podatkov, vključno z ustvarjanjem, shranjevanjem, združevanjem, osnutki, poročanjem, obveščanjem ali uničenjem, finančnega subjekta ne izpostavlja tveganjem.

POGLAVJE V

Obvladovanje tveganj tretjih strani na področju IKT

Oddelek I

Ključna načela za dobro obvladovanje tveganj tretjih strani na področju IKT

Člen 28

Splošna načela

1. Finančni subjekti obvladujejo tveganja tretjih strani na področju IKT kot sestavni del tveganj na področju IKT v sklopu okvira za obvladovanje tveganj na področju IKT iz člena 6(1) v skladu z naslednjimi načeli:

(a) finančni subjekti, ki imajo za vodenje svojih poslovnih dejavnosti sklenjene pogodbene dogovore za uporabo storitev IKT, so ves čas v celoti odgovorni za spoštovanje in izpolnjevanje vseh obveznosti iz te uredbe in veljavnega prava o finančnih storitvah;

(b) finančni subjekti obvladujejo tveganja tretjih strani na področju IKT glede na načelo sorazmernosti, pri čemer upoštevajo:

(i) naravo, obseg, zapletenost in pomen odvisnosti, povezanih z IKT;

(ii) tveganja, ki izhajajo iz pogodbenih dogovorov o uporabi storitev IKT, sklenjenih s tretjimi ponudniki storitev IKT, ob upoštevanju kritičnosti ali pomena posamezne storitve, postopka ali funkcije ter možnega učinka na neprekinjenost in dostopnost finančnih storitev in dejavnosti na individualni in skupinski ravni.

2. Finančni subjekti, ki niso subjekti iz člena 16(1), prvi pododstavek, in niso mikropodjetja, v sklopu svojega okvira za obvladovanje tveganj na področju IKT sprejmejo in redno pregledujejo strategijo o tveganju tretjih strani na področju IKT, pri čemer upoštevajo večdobaviteljsko strategijo iz člena 6(9), kadar je ustrezno. Strategija o tveganju tretjih strani na področju IKT vključuje politiko o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, ki jih opravljajo tretji ponudniki storitev IKT, in se uporablja na posamični podlagi in, kadar je ustrezno, na subkonsolidirani in konsolidirani podlagi. Upravljalni organ na podlagi ocene splošnega profila tveganja finančnega subjekta ter obsega in kompleksnosti njegovih poslovnih storitev redno pregleduje tveganja, identificirana v zvezi s pogodbenimi dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije.

3. Finančni subjekti v sklopu svojega okvira za obvladovanje tveganj na področju IKT na ravni subjekta ter na subkonsolidirani in konsolidirani ravni vzdržujejo in posodabljajo register informacij v zvezi z vsemi pogodbenimi dogovori o uporabi storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT.

Pogodbeni dogovori iz prvega pododstavka se ustrezno dokumentirajo, pri čemer se razlikuje med tistimi, ki zajemajo storitve IKT, ki podpirajo kritične ali pomembne funkcije, in tistimi, ki ne zajemajo takih funkcij.

Finančni subjekti pristojnim organom vsaj enkrat letno poročajo o številu novih dogovorov o uporabi storitev IKT, kategorijah tretjih ponudnikov storitev IKT, vrsti pogodbenih dogovorov ter storitvah in funkcijah IKT, ki se opravljajo.

Finančni subjekti pristojnemu organu na njegovo zahtevo predložijo celoten register informacij ali, kot se zahteva, določene oddelke registra, skupaj z vsemi informacijami, za katere se meni, da so potrebne za učinkovit nadzor finančnega subjekta.

Finančni subjekti pravočasno obvestijo pristojni organ o kakršnem koli načrtovanem pogodbenem dogovoru o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, in o tem, kdaj je funkcija postala kritična ali pomembna.

4. Finančni subjekti pred sklenitvijo pogodbenega dogovora o uporabi storitev IKT:

(a) ocenijo, ali pogodbeni dogovor zajema uporabo storitev IKT, ki podpirajo kritično ali pomembno funkcijo;

(b) ocenijo, ali so izpolnjeni nadzorni pogoji za sklenitev pogodbenega dogovora;

(c) identificirajo in ocenijo vsa pomembna tveganja v zvezi s pogodbenim dogovorom, vključno z možnostjo, da lahko tak pogodbeni dogovor prispeva k povečanju tveganja koncentracije na področju IKT iz člena 29;

(d) opravijo skrben pregled potencialnih tretjih ponudnikov storitev IKT in s postopki izbire in ocenjevanja zagotovijo ustreznost tretjega ponudnika storitev IKT;

(e) identificirajo in ocenijo nasprotja interesov, ki jih lahko povzroči pogodbeni dogovor.

5. Finančni subjekti lahko sklepajo pogodbene dogovore samo s tretjimi ponudniki storitev IKT, ki izpolnjujejo standarde informacijske varnosti. Kadar ti pogodbeni dogovori zadevajo kritične ali pomembne funkcije, finančni subjekti pred sklenitvijo dogovorov ustrezno upoštevajo, ali tretji ponudniki storitev IKT uporabljajo najnovejše in najkakovostnejše standarde informacijske varnosti.

6. Finančni subjekti pri uveljavljanju pravic do dostopa, inšpekcijskih pregledov in revizij pri tretjem ponudniku storitev IKT vnaprej določijo pogostost revizij in inšpekcijskih pregledov ter področja, ki jih je treba revidirati, na podlagi pristopa, ki temelji na tveganju, in ob upoštevanju splošno sprejetih revizijskih standardov v skladu z vsemi nadzornimi navodili o uporabi in vključitvi takih revizijskih standardov.

Kadar so pogodbeni dogovori o uporabi storitev IKT, sklenjeni s tretjimi ponudniki storitev IKT, tehnično zelo zapleteni, finančni subjekt preveri, ali imajo revizorji, ne glede na to, ali so to notranji ali zunanji revizorji oziroma skupine revizorjev, ustrezne spretnosti in znanje za učinkovito izvajanje ustreznih revizij in ocen.

7. Finančni subjekti zagotovijo, da se pogodbeni dogovori o uporabi storitev IKT lahko prekinejo v kateri koli od naslednjih okoliščin:

(a) znatna kršitev veljavnih zakonov, predpisov ali pogodbenih pogojev s strani tretjega ponudnika storitev IKT;

(b) okoliščine, identificirane med spremljanjem tveganja tretjih strani na področju IKT, za katere se šteje, da lahko spremenijo izvajanje funkcij, opravljenih na podlagi pogodbenega dogovora, vključno s pomembnimi spremembami, ki vplivajo na dogovor ali položaj tretjega ponudnika storitev IKT;

(c) dokazane šibkosti tretjega ponudnika storitev IKT v zvezi z njegovim splošnim obvladovanjem tveganj na področju IKT in zlasti v načinu, kako zagotavlja razpoložljivost, avtentičnost, celovitost in zaupnost podatkov, bodisi osebnih ali kako drugače občutljivih podatkov bodisi neosebnih podatkov;

(d) kadar pristojni organ zaradi pogojev zadevnega pogodbenega dogovora ali okoliščin v zvezi z njim ne more več učinkovito nadzirati finančnega subjekta.

8. Finančni subjekti vzpostavijo izhodne strategije za storitve IKT, ki podpirajo kritične ali pomembne funkcije. V izhodnih strategijah se upoštevajo tveganja, ki se lahko pojavijo na ravni tretjih ponudnikov storitev IKT, zlasti njihovo morebitno prenehanje delovanja, poslabšanje kakovosti opravljenih storitev IKT, kakršne koli motnje v poslovanju zaradi neprimernega ali neuspešnega opravljanja storitev ali kakršno koli pomembno tveganje, ki izhaja iz ustrezne in stalne uporabe zadevne storitve IKT, ali odpoved pogodbenih dogovorov s tretjimi ponudniki storitev IKT v kateri koli od okoliščin iz odstavka 7.

Finančni subjekti zagotovijo, da lahko prekinejo pogodbene dogovore brez:

(a) motenj svojih poslovnih dejavnosti;

(b) omejevanja skladnosti z zakonskimi zahtevami;

(c) škode za neprekinjenost in kakovost storitev, opravljenih za stranke.

Izhodni načrti morajo biti izčrpni, dokumentirani ter morajo biti v skladu z merili, določenimi v členu 4(2), zadostno testirani in redno pregledovani.

Finančni subjekti identificirajo alternativne rešitve in oblikujejo prehodne načrte, ki jim omogočajo, da tretjemu ponudniku storitev IKT odvzamejo pogodbene storitve IKT in ustrezne podatke ter jih varno in celovito prenesejo k alternativnim ponudnikom ali jih ponovno vključijo v lastno podjetje.

Finančni subjekti vzpostavijo ukrepe ob nepredvidljivih dogodkih za ohranitev neprekinjenosti poslovanja v primeru okoliščin iz prvega pododstavka.

9. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke izvedbenih tehničnih standardov za vzpostavitev standardnih predlog za namene registra informacij iz odstavka 3, vključno z informacijami, ki so skupne vsem pogodbenim dogovorom o uporabi storitev IKT. Evropski nadzorni organi te osnutke izvedbenih tehničnih standardov Komisiji predložijo do 17. januarja 2024.

Na Komisijo se prenese pooblastilo za sprejetje izvedbenih tehničnih standardov iz prvega pododstavka v skladu s členom 15 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

10. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih tehničnih standardov, da nadalje opredelijo podrobno vsebino politike iz odstavka 2 v zvezi s pogodbenimi dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, ki jih opravljajo tretji ponudniki storitev IKT.

Evropski nadzorni organi pri oblikovanju navedenih osnutkov regulativnih tehničnih standardov upoštevajo velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja. Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. januarja 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 29

Predhodna ocena tveganja koncentracije na področju IKT na ravni subjekta

1. Finančni subjekti pri identificiranju in ocenjevanju tveganj iz člena 28(4), točka (c), upoštevajo tudi, ali bi predvidena sklenitev pogodbenega dogovora v zvezi s storitvami IKT, ki podpirajo kritične ali pomembne funkcije, povzročila:

(a) sklenitev pogodbe s tretjim ponudnikom storitev IKT, ki ga ni enostavno nadomestiti, ali

(b) obstoj več pogodbenih dogovorov v zvezi z opravljanjem storitev IKT, ki podpirajo kritične ali pomembne funkcije, z istim tretjim ponudnikom storitev IKT ali tesno povezanimi tretjimi ponudniki storitev IKT.

Finančni subjekti pretehtajo koristi in stroške alternativnih rešitev, kot je uporaba različnih tretjih ponudnikov storitev IKT, pri čemer upoštevajo, ali in kako predvidene rešitve ustrezajo poslovnim potrebam in ciljem iz njihove strategije za digitalno odpornost.

2. Kadar pogodbeni dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, vključujejo možnost, da tretji ponudnik storitev IKT kritično ali pomembno funkcijo nadalje odda v podizvajanje drugim tretjim ponudnikom storitev IKT, finančni subjekti pretehtajo koristi in tveganja, ki lahko nastanejo v povezavi s tako morebitno oddajo v podizvajanje, zlasti v primeru podizvajalca storitev IKT s sedežem v tretji državi.

Kadar pogodbeni dogovori zadevajo storitve IKT, ki podpirajo kritične ali pomembne funkcije, finančni subjekti ustrezno upoštevajo določbe insolvenčnega prava, ki bi veljale v primeru stečaja tretjega ponudnika storitev IKT ter kakršno koli omejitev, ki se lahko pojavi v zvezi z nujno obnovitvijo podatkov finančnega subjekta.

Kadar se pogodbeni dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, sklenejo s tretjim ponudnikom storitev IKT s sedežem v tretji državi, finančni subjekti poleg dejavnikov iz drugega pododstavka upoštevajo še skladnost s pravili Unije o varstvu podatkov in učinkovitost izvrševanja prava v tej tretji državi.

Kadar pogodbeni dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, vključujejo možnost podizvajanja, finančni subjekti ocenijo, ali in kako lahko potencialno dolge ali zapletene verige podizvajanja vplivajo na njihovo zmožnost popolnega spremljanja pogodbenih funkcij in na zmožnost pristojnega organa, da v zvezi s tem učinkovito nadzoruje finančni subjekt.

Člen 30

Ključne pogodbene določbe

1. Pravice in obveznosti finančnega subjekta in tretjega ponudnika storitev IKT se jasno dodelijo in določijo v pisni obliki. Celotna pogodba vključuje sporazume o ravni storitve in se dokumentira v enem pisnem dokumentu, ki je na voljo strankam v papirni obliki ali v dokumentu druge oblike, ki jo je mogoče prenesti in trajna in dostopna.

2. V pogodbene dogovore o uporabi storitev IKT se vključijo vsaj naslednji elementi:

(a) jasen in popoln opis vseh funkcij in storitev IKT, ki jih mora opraviti tretji ponudnik storitev IKT, z navedbo, ali je dovoljeno oddajanje storitve IKT, ki podpira kritične ali pomembne funkcije, ali njenih bistvenih delov v podizvajanje in, če je dovoljeno, pogoje, ki veljajo za tako podizvajanje;

(b) lokacije, in sicer regije in države, kjer se opravljajo pogodbene funkcije in storitve IKT, oddane v izvajanje ali podizvajanje, in obdelovali podatki, vključno z lokacijo hrambe, ter zahtevo, da tretji ponudnik storitev IKT vnaprej obvesti finančni subjekt, če namerava spremeniti te lokacije;

(c) določbe o razpoložljivosti, avtentičnosti, celovitosti in zaupnosti v zvezi z varstvom podatkov, vključno z osebnimi podatki;

(d) določbe o zagotavljanju dostopa, obnovitve in restavriranja osebnih in neosebnih podatkov v preprosto dostopni obliki, ki jih obdeluje finančni subjekt, v primeru insolventnosti, reševanja ali prenehanja poslovanja tretjega ponudnika storitev IKT ali v primeru odpovedi pogodbenih dogovorov;

(e) opisi ravni storitev, vključno z njihovimi posodobitvami in popravki;

(f) obveznost tretjega ponudnika storitev IKT, da v primeru incidenta, povezanega z IKT in s storitvijo IKT, ki se opravi za finančni subjekt, temu zagotovi pomoč brez dodatnih stroškov ali po predhodno določeni ceni;

(g) obveznost tretjega ponudnika storitev, da v celoti sodeluje s pristojnimi organi in organi za reševanje finančnega subjekta, vključno z osebami, ki jih ti imenujejo;

(h) pravice do odpovedi in povezani minimalni roki za odpoved pogodbenih dogovorov v skladu s pričakovanji pristojnih organov in organov za reševanje;

(i) pogoji sodelovanja tretjih ponudnikov storitev IKT v programih ozaveščanja o varnosti na področju IKT in usposabljanju na področju digitalne operativne odpornosti finančnih subjektov, v skladu s členom 13(6).

3. V pogodbene dogovore o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, se poleg elementov iz odstavka 2 vključi vsaj naslednje:

(a) celoviti opisi ravni storitev – tudi njihove posodobitve in popravki –, v katerih so določeni natančni kvantitativni in kvalitativni cilji uspešnosti znotraj dogovorjenih ravni storitev, da lahko finančni subjekt učinkovito spremlja storitve IKT in omogoči sprejetje ustreznih popravnih ukrepov brez nepotrebnega odlašanja, ko dogovorjene ravni storitev niso dosežene;

(b) odpovedni roki in obveznosti tretjega ponudnika storitev IKT za poročanje finančnemu subjektu, vključno z obveščanjem o spremembah, ki bi lahko pomembno vplivale na zmožnost tretjega ponudnika storitev IKT, da učinkovito opravlja storitve IKT, ki podpirajo kritične ali pomembne funkcije v skladu z dogovorjenimi ravnmi storitev;

(c) zahteve, da tretji ponudnik storitev IKT izvaja in testira poslovne načrte izrednih ukrepov ter vzpostavi varnostne ukrepe, orodja in politike na področju IKT, ki finančnemu subjektu zagotavljajo ustrezno raven varnosti za opravljanje storitev v skladu z njegovim regulativnim okvirom;

(d) obveznost tretjega ponudnika storitev IKT, da sodeluje in se v celoti udejstvuje pri penetracijskem testu na podlagi groženj, kot je navedeno v členih 26 in 27;

(e) pravica do stalnega spremljanja uspešnosti tretjega ponudnika storitev IKT, ki vključuje naslednje:

(i) neomejene pravice do dostopa, inšpekcijskega pregleda in revizije s strani finančnega subjekta ali imenovane tretje strani in pristojnega organa ter pravico, da pridobijo kopije ustrezne dokumentacije na kraju samem, če so kritične za poslovanje tretjih ponudnikov storitev IKT, pri čemer drugi pogodbeni dogovori ali izvedbene politike ne ovirajo ali omejujejo učinkovitega uveljavljanja teh pravic;

(ii) pravico, da se zahtevajo alternativne ravni zanesljivosti, če so prizadete pravice drugih strank;

(iii) obveznost tretjega ponudnika storitev IKT, da bo v celoti sodeloval pri inšpekcijskih pregledih in revizijah na kraju samem, ki jih izvajajo pristojni organi, glavni nadzornik, finančni subjekt ali imenovana tretja stran, ter

(iv) obveznost, da predloži podrobnosti o obsegu, zahtevanih postopkih in pogostosti teh inšpekcijskih pregledov in revizij;

(f) izhodne strategije, zlasti določitev obveznega ustreznega prehodnega obdobja:

(i) med katerim bo tretji ponudnik storitev IKT še naprej opravljal ustrezne funkcije ali storitve IKT, da bi zmanjšal tveganje motenj pri finančnem subjektu ali zagotovil njihovo učinkovito reševanje in prestrukturiranje;

(ii) ki finančnemu subjektu omogoča, da preide na drugega tretjega ponudnika storitev IKT ali na rešitve v okviru lastnega podjetja, ki so skladne s kompleksnostjo opravljene storitve.

Z odstopanjem od točke (e) se lahko tretji ponudnik storitev IKT in finančni subjekt, ki je mikropodjetje, dogovorita, da se lahko pravice finančnega subjekta do dostopa, inšpekcijskega pregleda in revizije prenesejo na neodvisno tretjo stran, ki jo imenuje tretji ponudnik storitev IKT, finančni subjekt pa lahko od tretje strani kadar koli zahteva informacije in zagotovila glede uspešnosti tretjega ponudnika storitev IKT.

4. Pri pogajanjih o pogodbenih dogovorih finančni subjekti in tretji ponudniki storitev IKT upoštevajo uporabo standardnih pogodbenih klavzul, ki jih javni organi oblikujejo za določene storitve.

5. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih tehničnih standardov, da natančneje opredelijo elemente iz odstavka 2, točka (a), ki jih mora finančni subjekt določiti in oceniti pri oddaji storitev IKT, ki podpirajo kritične ali pomembne funkcije, v podizvajanje.

Evropski nadzorni organi pri oblikovanju navedenih osnutkov regulativnih tehničnih standardov upoštevajo velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predloži do 17. julija 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Oddelek II

Okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT

Člen 31

Imenovanje ključnih tretjih ponudnikov storitev IKT

1. Evropski nadzorni organi prek Skupnega odbora in na podlagi priporočila nadzorniškega foruma, ustanovljenega v skladu s členom 32(1):

(a) imenujejo tretje ponudnike storitev IKT, ki so ključni za finančne subjekte, in sicer na podlagi ocene, pri kateri se upoštevajo merila iz odstavka 2;

(b) kot glavnega nadzornika za vsakega ključnega tretjega ponudnika storitev IKT imenujejo evropski nadzorni organ, ki je v skladu z uredbami (EU) št. 1093/2010, (EU) št. 1094/2010 ali (EU) št. 1095/2010 odgovoren za finančne subjekte, ki imajo skupno največji delež celotnih sredstev glede na vrednost celotnih sredstev vseh finančnih subjektov, ki uporabljajo storitve zadevnega ključnega tretjega ponudnika storitev IKT, kar dokazuje vsota posameznih bilanc stanja navedenih finančnih subjektov.

2. Imenovanje iz odstavka 1, točka (a), temelji na vseh naslednjih merilih v zvezi s storitvami IKT, ki jih opravlja tretji ponudnik storitev IKT:

(a) sistemski učinek na stabilnost, neprekinjenost ali kakovost opravljanja finančnih storitev v primeru, da bi se zadevni tretji ponudnik storitev IKT soočal z obsežno motnjo v delovanju pri opravljanju svojih storitev, ob upoštevanju števila finančnih subjektov in skupne vrednosti sredstev finančnih subjektov, za katere zadevni tretji ponudnik storitev IKT opravlja storitve;

(b) sistemski značaj ali pomen finančnih subjektov, ki so odvisni od zadevnega tretjega ponudnika storitev IKT, ocenjen v skladu z naslednjimi parametri:

(i) število globalnih sistemsko pomembnih institucij ali drugih sistemsko pomembnih institucij, ki so odvisne od zadevnega tretjega ponudnika storitev IKT;

(ii) soodvisnost med globalnimi sistemsko pomembnimi institucijami ali drugimi sistemsko pomembnimi institucijami iz točke (i) in drugimi finančnimi subjekti, vključno s situacijami, ko globalne sistemsko pomembne institucije ali druge sistemsko pomembne institucije za druge finančne subjekte opravljajo storitve finančne infrastrukture;

(c) odvisnost finančnih subjektov od storitev, ki jih opravlja zadevni tretji ponudnik storitev IKT v zvezi s kritičnimi ali pomembnimi funkcijami finančnih subjektov, ki nazadnje vključujejo istega tretjega ponudnika storitev IKT, ne glede na to, ali so finančni subjekti od teh storitev odvisni neposredno ali posredno, na podlagi dogovorov o podizvajanju;

(d) stopnja nadomestljivosti tretjega ponudnika storitev IKT, ob upoštevanju naslednjih parametrov:

(i) pomanjkanje resničnih alternativ, celo delnih, zaradi omejenega števila tretjih ponudnikov storitev IKT, ki delujejo na določenem trgu, ali tržnega deleža zadevnega tretjega ponudnika storitev IKT ali zaradi obstoječe tehnične zapletenosti ali izpopolnjenosti, tudi v zvezi s kakršno koli zaščiteno tehnologijo ali posebnostmi organizacije ali dejavnosti tretjega ponudnika storitev IKT;

(ii) težave v zvezi z delno ali popolno selitvijo ustreznih podatkov in delovnih obremenitev z zadevnega tretjega ponudnika storitev IKT na drugega tretjega ponudnika storitev IKT, bodisi zaradi znatnih finančnih stroškov, časa ali drugih virov, ki jih lahko povzroči postopek selitve, bodisi zaradi povečanega tveganja na področju IKT ali drugih operativnih tveganj, ki jim je finančni subjekt lahko izpostavljen s tako selitvijo.

3. Kadar je tretji ponudnik storitev IKT del skupine, se merila iz odstavka 2 upoštevajo v zvezi s storitvami IKT, ki jih opravlja skupina kot celota.

4. Za lažjo komunikacijo z glavnim nadzornikom in zagotovitev ustrezne zastopanosti ključni tretji ponudniki storitev IKT, ki so del skupine, za svojo koordinacijsko točko imenujejo eno pravno osebo.

5. Glavni nadzornik obvesti tretjega ponudnika storitev IKT o rezultatih ocene, ki je podlaga za imenovanje iz odstavka 1, točka (a). Tretji ponudnik storitev IKT lahko v šestih tednih od datuma obvestila glavnemu nadzorniku predloži utemeljeno izjavo z vsemi ustreznimi informacijami za namene ocene. Glavni nadzornik preuči utemeljeno izjavo in lahko zahteva predložitev dodatnih informacij v 30 koledarskih dneh od prejema te izjave.

Potem ko evropski nadzorni organi prek Skupnega odbora tretjega ponudnika storitev IKT imenuje za ključnega ponudnika, o tem imenovanju in datumu začetka, od katerega bo dejansko predmet nadzornih dejavnosti, obvestijo tretjega ponudnika storitev IKT. Datum začetka nastopi najpozneje en mesec po obvestilu. Tretji ponudnik storitev IKT obvesti finančne subjekte, za katere opravlja storitve, da je imenovan za ključnega ponudnika.

6. Na Komisijo se prenese pooblastilo, da do 17. julija 2024 sprejme delegirani akt v skladu s členom 57 za dopolnitev te uredbe z nadaljnjo opredelitvijo meril iz odstavka 2 tega člena.

7. Imenovanje iz odstavka 1, točka (a), se ne uporablja, dokler Komisija ne sprejme delegiranega akta v skladu z odstavkom 6.

8. Imenovanje iz odstavka 1, točka (a), ne velja za naslednje:

(i) finančne subjekte, ki opravljajo storitve IKT za druge finančne subjekte;

(ii) tretje ponudnike storitev IKT, za katere veljajo okviri nadzora, vzpostavljeni za namene podpiranja nalog iz člena 127(2) Pogodbe o delovanju Evropske unije;

(iii) tretje ponudnike storitev IKT znotraj skupine;

(iv) tretje ponudnike storitev IKT, ki storitve IKT opravljajo samo v eni državi članici za finančne subjekte, ki so dejavni samo v tej državi članici.

9. Evropski nadzorni organi prek Skupnega odbora vsako leto pripravijo, objavijo in posodobijo seznam ključnih tretjih ponudnikov storitev IKT na ravni Unije.

10. Za namene odstavka 1, točka (a), pristojni organi na letni in zbirni ravni pošljejo poročila iz člena 28(3), tretji pododstavek, nadzorniškemu forumu, ustanovljenemu na podlagi člena 32. Nadzorniški forum na podlagi informacij, ki jih prejme od pristojnih organov, oceni odvisnosti finančnih subjektov od tretjih strani na področju IKT.

11. Tretji ponudniki storitev IKT, ki niso vključeni na seznam iz odstavka 9, lahko zaprosijo, da se jih imenuje za ključne ponudnike v skladu z odstavkom 1, točka (a).

Za namene prvega pododstavka tretji ponudnik storitev IKT predloži utemeljeno zahtevo EBA, ESMA ali EIOPA, ki se prek Skupnega odbora odloči, ali bo navedenega tretjega ponudnika storitev IKT imenoval za ključnega ponudnika v skladu z odstavkom 1, točka (a).

Odločitev iz drugega pododstavka se sprejme in sporoči tretjemu ponudniku storitev IKT v šestih mesecih po prejemu vloge.

12. Finančni subjekti smejo uporabljati samo storitve tretjega ponudnika storitev IKT s sedežem v tretji državi, ki je bil imenovan za ključnega v skladu z odstavkom 1, točka (a), če je ta v 12 mesecih po imenovanju v Uniji ustanovil odvisno podjetje.

13. Ključni tretji ponudnik storitev IKT iz odstavka 12 uradno obvesti glavnega nadzornika o vseh spremembah strukture upravljanja odvisnega podjetja, ustanovljenega v Uniji.

Člen 32

Struktura okvira nadzora

1. Skupni odbor v skladu s členom 57(1) uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 ustanovi nadzorniški forum kot pododbor, ki podpira naloge Skupnega odbora in glavnega nadzornika iz člena 31(1), točka (b), na področju tveganj tretjih strani na področju IKT v finančnih sektorjih. Nadzorniški forum pripravi osnutke skupnih stališč in osnutke skupnih aktov Skupnega odbora na navedenem področju.

Nadzorniški forum redno razpravlja o relevantnih spremembah pri tveganjih in ranljivostih na področju IKT ter spodbuja dosleden pristop pri spremljanju tveganja tretjih strani na področju IKT na ravni Unije.

2. Nadzorniški forum enkrat letno opravi kolektivno oceno rezultatov in ugotovitev nadzornih dejavnosti, ki se izvajajo za vse ključne tretje ponudnike storitev IKT, in spodbuja usklajevalne ukrepe za povečanje digitalne operativne odpornosti finančnih subjektov ter spodbujanje najboljših praks pri obravnavanju tveganj koncentracije na področju IKT in raziskovanje načinov za zmanjševanje tveganja za medsektorske prenose tveganja.

3. Nadzorniški forum predloži izčrpne referenčne vrednosti za ključne tretje ponudnike storitev IKT, ki jih Skupni odbor sprejme kot skupna stališča evropskih nadzornih organov v skladu s členom 56(1) uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

4. Nadzorniški forum sestavljajo:

(a) predsedniki evropskih nadzornih organov;

(b) en predstavnik na visoki ravni, ki je izbran med osebjem, zaposlenim v ustreznem pristojnem organu iz člena 46 iz vsake države članice;

(c) izvršni direktorji vsakega evropskega nadzornega organa in po en predstavnik Komisije ter ESRB, ECB in ENISA v vlogi opazovalcev;

(d) po potrebi dodatni predstavnik pristojnega organa iz člena 46 iz vsake države članice v vlogi opazovalca;

(e) kot je ustrezno, predstavnik pristojnih organov, imenovanih ali vzpostavljenih v skladu z Direktivo (EU) 2022/2555, odgovornih za nadzor nad bistvenim ali pomembnim subjektom, za katere velja navedena direktiva, ki je bil imenovan za ključnega tretjega ponudnika storitev IKT, v vlogi opazovalca.

Nadzorniški forum se lahko po potrebi posvetuje z neodvisnimi strokovnjaki, imenovanimi v skladu z odstavkom 6.

5. Vsaka država članica imenuje ustrezni pristojni organ, katerega član osebja je predstavnik na visoki ravni iz odstavka 4, prvi pododstavek, točka (b), in o tem obvesti glavnega nadzornika.

Evropski nadzorni organi na svojem spletnem mestu objavijo seznam predstavnikov na visoki ravni, izbranih med osebjem, zaposlenim v ustreznem pristojnem organu, ki jih imenujejo države članice.

6. Neodvisne strokovnjake iz odstavka 4, drugi pododstavek, imenuje nadzorniški forum, ki jih na podlagi javnega in preglednega postopka prijave izbere iz nabora strokovnjakov.

Neodvisni strokovnjaki so imenovani na podlagi strokovnega znanja o finančni stabilnosti, digitalni operativni odpornosti in varnostnih vprašanjih na področju IKT. Delujejo neodvisno in objektivno, izključno v interesu Unije kot celote ter ne zahtevajo in ne sprejemajo navodil institucij ali organov Unije, katere koli vlade države članice ali katerih koli drugih javnih ali zasebnih organov.

7. Evropski nadzorni organi v skladu s členom 16 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 do 17. julija 2024 za namene tega oddelka izdajo smernice o sodelovanju med evropskimi nadzornimi organi in pristojnimi organi, ki zajemajo podrobne postopke in pogoje za razdelitev in izvajanje nalog med pristojnimi organi in evropskimi nadzornimi organi ter podrobnosti glede izmenjave informacij, ki so potrebne, da organi zagotovijo nadaljnje ukrepanje na podlagi priporočil iz člena 35(1), točka (d), naslovljeno na ključne tretje ponudnike storitev IKT.

8. Zahteve iz tega oddelka ne posegajo v uporabo Direktive (EU) 2022/2555 in drugih pravil Unije o nadzoru, ki veljajo za ponudnike storitev računalništva v oblaku.

9. Evropski nadzorni organi prek Skupnega odbora in na podlagi pripravljalnega dela, ki ga izvede nadzorniški forum, enkrat letno predložijo poročilo o uporabi tega oddelka Evropskemu parlamentu, Svetu in Komisiji.

Člen 33

Naloge glavnega nadzornika

1. Glavni nadzornik, imenovan v skladu s členom 31(1), točka (b), izvaja nadzor nad ključnimi tretjimi ponudniki storitev IKT, ki so mu dodeljeni, in je zanje glavna kontaktna točka za vsa vprašanja, povezana z nadzorom.

2. Za namene odstavka 1 glavni nadzornik oceni, ali ima vsak ključni tretji ponudnik storitev IKT vzpostavljena celovita, zanesljiva in učinkovita pravila, postopke, mehanizme in dogovore za obvladovanje tveganj na področju IKT, ki jih lahko predstavlja za finančne subjekte.

Ocena iz prvega pododstavka se osredotoči predvsem na storitve IKT, ki jih opravljajo ključni tretji ponudnik storitev IKT ter ki podpirajo kritične ali pomembne funkcije finančnih subjektov. Kadar je potrebno za obravnavanje vseh relevantnih tveganj, se ta ocena razširi na storitve IKT, ki podpirajo tudi funkcije, ki niso kritične ali pomembne funkcije.

3. Ocena iz odstavka 2 zajema:

(a) zahteve v zvezi IKT, da se zagotovijo zlasti varnost, razpoložljivost, neprekinjenost, nadgradljivost in kakovost storitev, ki jih ključni tretji ponudnik storitev IKT zagotavlja finančnim subjektom, ter zmožnost stalnega ohranjanja visokih standardov glede razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti podatkov;

(b) fizično varnost, ki prispeva k zagotavljanju varnosti IKT, vključno z varnostjo prostorov, objektov in podatkovnih centrov;

(c) postopke obvladovanja tveganj, vključno s politikami obvladovanja tveganj na področju IKT, politiko neprekinjenega poslovanja na področju IKT ter načrti odzivanja in okrevanja IKT;

(d) ureditve upravljanja, vključno z organizacijsko strukturo z jasnimi, preglednimi in doslednimi opredelitvami pristojnosti in odgovornosti, ki omogočajo učinkovito obvladovanje tveganj na področju IKT;

(e) identificiranje in spremljanje pomembnejših incidentov, povezanih z IKT, takojšnje poročanje finančnim subjektom o njih ter obvladovanje in reševanje teh incidentov, zlasti kibernetskih napadov;

(f) mehanizme za prenosljivost podatkov, prenosljivost aplikacij in interoperabilnost, ki finančnim subjektom zagotavljajo učinkovito uveljavljanje pravic do odpovedi;

(g) testiranje sistemov, infrastrukture in kontrol IKT;

(h) revizije IKT;

(i) uporabo ustreznih nacionalnih in mednarodnih standardov, ki se uporabljajo za opravljanje ponudnikovih storitev IKT finančnim subjektom.

4. Glavni nadzornik na podlagi ocene iz odstavka 2 in ob usklajevanju s skupno nadzorno mrežo iz člena 34(1) sprejme jasen, podroben in obrazložen individualni načrt nadzora za vsakega ključnega tretjega ponudnika storitev IKT z opisom letnih ciljev in glavnih načrtovanih ukrepov v zvezi z nadzorom. Ta načrt se vsako leto posreduje ključnemu tretjemu ponudniku storitev IKT.

Glavni nadzornik pred sprejetjem načrta nadzora ključnemu tretjemu ponudniku storitev IKT posreduje njegov osnutek.

Ključni tretji ponudnik storitev IKT lahko po prejemu osnutka načrta nadzora v 15 koledarskih dneh predloži utemeljeno izjavo, v kateri dokumentira pričakovani učinek na stranke, ki niso subjekti, ki spadajo na področje uporabe te uredbe, in po potrebi predstavi rešitve za zmanjšanje tveganj.

5. Ko so letni načrti nadzora iz odstavka 4 sprejeti in so ključni tretji ponudniki storitev IKT o njih obveščeni, lahko pristojni organi sprejmejo ukrepe v zvezi s takimi ključnimi tretjimi ponudniki storitev IKT samo v dogovoru z glavnim nadzornikom.

Člen 34

Operativno usklajevanje med glavnimi nadzorniki

1. Da bi se zagotovil dosleden pristop k nadzornim dejavnostim ter omogočili usklajene splošne nadzorne strategije in skladni operativni pristopi in delovne metodologije, trije glavni nadzorniki, imenovani v skladu s členom 31(1), točka (b), vzpostavijo skupno nadzorno mrežo, da se med seboj usklajujejo v pripravljalnih fazah in usklajujejo izvajanje dejavnosti nadzora nad ključnimi tretjimi ponudniki storitev IKT, za katere so pristojni, kot tudi o vseh ukrepih, ki bi lahko bili potrebni na podlagi člena 42.

2. Za namene odstavka 1 glavni nadzorniki pripravijo skupni protokol o nadzoru, v katerem določijo podrobne postopke, ki jih je treba upoštevati pri vsakodnevnem usklajevanju ter pri zagotavljanju hitrih izmenjav in odzivov. Protokol se redno revidira, da se upoštevajo operativne potrebe, zlasti razvoj praktičnih ureditev nadzora.

3. Glavni nadzorniki lahko priložnostno zaprosijo ECB in ENISA za tehnični nasvet, izmenjavo praktičnih izkušenj ali sodelovanje na posebnih usklajevalnih sestankih skupne nadzorne mreže.

Člen 35

Pooblastila glavnega nadzornika

1. Za namene izvajanja nalog, določenih v tem oddelku, ima glavni nadzornik v zvezi s ključnimi tretjimi ponudniki storitev IKT naslednja pooblastila:

(a) da zahteva vse ustrezne informacije in dokumentacijo v skladu s členom 37;

(b) da izvaja splošne preiskave in inšpekcijske preglede v skladu s členom 38 oziroma členom 39;

(c) da po zaključku nadzornih dejavnosti zahteva poročila, v katerih so navedeni sprejeti ukrepi ali popravni ukrepi, ki so jih izvedli ključni tretji ponudniki storitev IKT v zvezi s priporočili iz točke (d) tega odstavka;

(d) da izda priporočila na področjih iz člena 33(3), zlasti glede:

(i) uporabe posebnih zahtev ali postopkov glede kakovosti in varnosti IKT, zlasti v zvezi z uvedbo popravkov, posodobitev, šifriranja in drugih varnostnih ukrepov, za katere glavni nadzornik meni, da so pomembni za zagotavljanje varnosti storitev na področju IKT, ki se zagotavljajo finančnim subjektom;

(ii) uporabe pogojev, vključno z njihovo tehnično izvedbo, pod katerimi ključni tretji ponudniki storitev IKT zagotavljajo storitve IKT finančnim subjektom in za katere glavni nadzornik meni, da so pomembni za preprečevanje nastanka ali povečanja kritičnih točk odpovedi ali za zmanjšanje možnih sistemskih učinkov na finančni sektor Unije v primeru tveganja koncentracije na področju IKT;

(iii) vsake načrtovane oddaje v podizvajanje, kadar glavni nadzornik na podlagi informacij, zbranih v skladu s členoma 37 in 38, meni, da lahko nadaljnje podizvajanje, vključno z dogovori o podizvajanju, ki jih nameravajo ključni tretji ponudniki storitev IKT skleniti z drugimi tretjimi ponudniki storitev IKT ali podizvajalci storitev IKT s sedežem v tretji državi, povzroči tveganje za opravljanje storitev s strani finančnega subjekta ali za finančno stabilnost;

(iv) opustitve sklepanja nadaljnjih dogovorov o podizvajanju, kadar so izpolnjeni naslednji kumulativni pogoji:

— predvideni podizvajalec je tretji ponudnik storitev IKT ali podizvajalec storitev IKT s sedežem v tretji državi;

— oddaja v podizvajanje se nanaša na kritično ali pomembno funkcijo finančnega subjekta ter

— glavni nadzornik meni, da taka oddaja v podizvajanje predstavlja jasno in resno tveganje za finančno stabilnost Unije ali za finančne subjekte, med drugim zmožnost finančnih subjektov, da izpolnijo zahteve v zvezi z nadzorom.

Za namene točke (iv) te točke tretji ponudniki storitev IKT glavnemu nadzorniku pošljejo informacije v zvezi z oddajo v podizvajanje, pri čemer uporabijo predlogo iz člena 41(1), točka (b).

2. Glavni nadzornik pri izvajanju pooblastil iz tega člena:

(a) zagotavlja redno usklajevanje v okviru skupne nadzorne mreže in si po potrebi zlasti prizadeva za dosledne pristope pri nadzoru ključnih tretjih ponudnikov storitev IKT;

(b) ustrezno upošteva okvir, vzpostavljen z Direktivo (EU) 2022/2555, in se po potrebi posvetuje z ustreznimi pristojnimi organi, imenovanimi ali vzpostavljenimi v skladu z navedeno direktivo, da se prepreči podvajanje tehničnih in organizacijskih ukrepov, ki bi se lahko uporabljali za ključne tretje ponudnike storitev IKT na podlagi navedene direktivo;

(c) poskuša čim bolj zmanjšati tveganje motenj pri storitvah, ki jih ključni tretji ponudniki storitev IKT zagotavljajo strankam, ki niso subjekti, ki spadajo na področje uporabe te uredbe.

3. Glavni nadzornik se pred izvrševanjem pooblastil iz odstavka 1 posvetuje z nadzorniškim forumom.

Pred izdajo priporočil v skladu z odstavkom 1, točka (d), glavni nadzornik tretjemu ponudniku storitev IKT omogoči, da v 30 koledarskih dneh predloži ustrezne informacije, ki dokazujejo pričakovani učinek na stranke, ki niso subjekti, ki spadajo na področje uporabe te uredbe, in po potrebi predstavi rešitve za blažitev tveganj.

4. Glavni nadzornik o izidu izvrševanja pooblastil iz odstavka 1, točki (a) in (b), obvesti skupno nadzorno mrežo. Glavni nadzornik poročila iz odstavka 1, točka (c), brez nepotrebnega odlašanja posreduje skupni nadzorni mreži in pristojnim organom finančnih subjektov, ki uporabljajo storitve IKT tega ključnega tretjega ponudnika storitev IKT.

5. Ključni tretji ponudniki storitev IKT v dobri veri sodelujejo z glavnim nadzornikom in mu pomagajo pri izpolnjevanju njegovih nalog.

6. Glavni nadzornik v primeru popolnega ali delnega neizpolnjevanja ukrepov, ki jih je treba sprejeti na podlagi izvrševanja pooblastil iz odstavka 1, točke (a), (b) in (c), in po izteku najmanj 30 koledarskih dni od datuma, ko je ključni tretji ponudnik storitev IKT prejel obvestilo o zadevnih ukrepih, sprejme odločitev o periodični denarni kazni, ki jo naloži ključnemu tretjemu ponudniku storitev IKT, da ga prisili k izpolnjevanju teh ukrepov.

7. Periodična denarna kazen iz odstavka 6 se naloži za vsak dan, dokler ni zagotovljeno izpolnjevanje ukrepov, vendar največ za šestmesečno obdobje po tem, ko je bil ključni tretji ponudnik storitev IKT obveščen o odločitvi, da se naloži periodična denarna kazen.

8. Znesek periodične denarne kazni, izračunan od datuma, določenega v odločbi o naložitvi periodične denarne kazni, je največ 1 % povprečnega dnevnega svetovnega prometa ključnega tretjega ponudnika storitev IKT v prejšnjem poslovnem letu. Glavni nadzornik pri določanju zneska denarne kazni upošteva naslednja merila v zvezi z neizpolnjevanjem ukrepov iz odstavka 6:

(a) resnost in trajanje neskladnosti;

(b) ali je neskladnost storjena namerno ali iz malomarnosti;

(c) raven sodelovanja tretjega ponudnika storitev IKT z glavnim nadzornikom.

Za namene prvega pododstavka in za zagotovitev doslednega pristopa se glavni nadzornik posvetuje s skupno nadzorno mrežo.

9. Denarna kazen je upravne narave in je izvršljiva. Izvršbo urejajo pravila civilnega postopka, ki veljajo v državi članici, na ozemlju katere se izvajajo inšpekcijski pregledi in obiski. Sodišča zadevne države članice so pristojna za pritožbe v zvezi z nepravilnim izvajanjem izvrševanja. Zneski denarnih kazni se dodelijo splošnemu proračunu Evropske unije.

10. Glavni nadzornik javnosti razkrije vsako periodično denarno kazen, ki je bila naložena, razen če bi tako razkritje resno ogrozilo finančne trge ali povzročilo nesorazmerno škodo udeleženim stranem.

11. Pred naložitvijo periodične denarne kazni iz odstavka 6 da glavni nadzornik predstavnikom ključnega tretjega ponudnika storitev IKT, v zvezi s katerim teče postopek, možnost, da podajo izjavo glede ugotovitev, in svoje odločitve utemelji le na ugotovitvah, na katere je imel ključni tretji ponudnik storitev IKT, ki je predmet postopke, priložnost podati pripombe.

V postopku se v celoti spoštujejo pravice do obrambe oseb, v zvezi s katerimi teče postopek. Ključni tretji ponudnik storitev IKT, v zvezi s katerim teče postopek, je upravičen do vpogleda v spis, ob upoštevanju zakonitega interesa drugih oseb za zaščito njihovih poslovnih skrivnosti. Pravica dostopa do spisa ne velja za zaupne informacije ali notranje pripravljalne dokumente glavnega nadzornika.

Člen 36

Izvrševanje pooblastil glavnega nadzornika zunaj Unije

1. Kadar ciljev nadzora ni mogoče doseči v sodelovanju z odvisnim podjetjem, ustanovljenim za namene člena 31(12), ali z izvajanjem nadzornih dejavnosti v prostorih, ki se nahajajo v Uniji, lahko glavni nadzornik v vseh prostorih v tretji državi, ki jih ima ključni tretji ponudnik storitev IKT v lasti ali jih na kakršen koli način uporablja za opravljanje storitev finančnim subjektom Unije, vključno z vsemi upravnimi, poslovnimi ali operativnimi uradi, prostori, zemljišči, zgradbami ali drugimi nepremičninami, v povezavi z njegovimi poslovnimi dejavnostmi, funkcijami ali storitvami izvršuje pooblastila iz naslednjih določb:

(a) člen 35(1), točka (a), in

(b) člen 35(1), točka (b), v skladu s členom 38(2), točke (a), (b) in (d), ter členom 39(1) in (2), točka (a).

Pooblastila iz prvega pododstavka se lahko izvršujejo ob upoštevanju vseh naslednjih pogojev:

(i) glavni nadzornik meni, da je izvedba inšpekcijskega pregleda v tretji državi potrebna, da lahko v celoti in učinkovito izvaja svoje naloge na podlagi te uredbe;

(ii) inšpekcijski pregled v tretji državi je neposredno povezan z opravljanjem storitev IKT za finančne subjekte v Uniji;

(iii) zadevni ključni tretji ponudnik storitev IKT soglaša z izvedbo inšpekcijskega pregleda v tretji državi in

(iv) ustrezni organ zadevne tretje države je bil uradno obveščen s strani glavnega nadzornika in ni nasprotoval.

2. EBA, ESMA ali EIOPA brez poseganja v pristojnosti institucij Unije oziroma držav članic za namene odstavka 1 sklenejo dogovore o upravnem sodelovanju z ustreznim organom tretje države, da se glavnemu nadzorniku in ekipi, imenovani za izvajanje njegovih nalog v zadevni tretji državi, omogoči nemoteno izvajanje inšpekcijskih pregledov v zadevni tretji državi. Ti dogovori o sodelovanju ne ustvarjajo pravnih obveznosti za Unijo in njene države članice niti državam članicam in njihovim pristojnim organom ne preprečujejo sklepanja dvostranskih ali večstranskih dogovorov z zadevnimi tretjimi državami in njihovimi ustreznimi organi.

V okviru teh dogovorov o sodelovanju se določijo vsaj naslednji elementi:

(a) postopki za usklajevanje nadzornih dejavnosti, ki se izvajajo na podlagi te uredbe, in kakršno koli podobno spremljanje tveganja tretjih strani na področju IKT v finančnem sektorju, ki ga izvaja ustrezni organ zadevne tretje države, vključno s podrobnostmi o posredovanju njegovega soglasja k temu, da se glavnemu nadzorniku in njegovi imenovani ekipi omogoči izvajanje splošnih preiskav in inšpekcijskih pregledov na kraju samem iz odstavka 1, prvi pododstavek, na ozemlju pod njeno jurisdikcijo;

(b) mehanizem za posredovanje vseh pomembnih informacij med EBA, ESMA ali EIOPA in ustreznim organom zadevne tretje države, zlasti v zvezi z informacijami, ki jih lahko zahteva glavni nadzornik na podlagi člena 37;

(c) mehanizme, s katerimi ustrezni organ zadevne tretje države takoj obvesti EBA, ESMA ali EIOPA o primerih, v katerih se šteje, da je tretji ponudnik storitev IKT s sedežem v tretji državi, ki je imenovan kot ključni ponudnik v skladu s členom 31(1), točka (a), kršil zahteve, ki jih mora v skladu z veljavnim pravom zadevne tretje države upoštevati pri opravljanju storitev za finančne institucije v tej tretji državi, ter uporabljena pravna sredstva in sankcije;

(d) redno posredovanje najnovejših informacij o regulativnem ali nadzornem razvoju v zvezi s spremljanjem tveganja na področju IKT, ki ga za finančne institucije v zadevni tretji državi predstavljajo tretje strani;

(e) podrobnosti, na podlagi katerih se po potrebi omogoči sodelovanje enega predstavnika ustreznega organa tretje države pri inšpekcijskih pregledih, ki jih izvajata glavni nadzornik in imenovana ekipa.

3. Glavni nadzornik v primeru, da ne more izvajati nadzornih dejavnosti iz odstavkov 1 in 2 zunaj Unije:

(a) izvaja svoja pooblastila iz člena 35 na podlagi vseh dejstev in dokumentov, ki jih ima na voljo;

(b) dokumentira in pojasni vse posledice nezmožnosti izvajanja predvidenih nadzornih dejavnosti iz tega člena.

Morebitne posledice iz točke (b) tega odstavka se upoštevajo v priporočilih glavnega nadzornika, izdanih na podlagi člena 35(1), točka (d).

Člen 37

Zahteva po predložitvi informacij

1. Glavni nadzornik lahko s preprostim zahtevkom ali sklepom zahteva, da ključni tretji ponudniki storitev IKT zagotovijo vse informacije, ki jih potrebuje za opravljanje svojih nalog na podlagi te uredbe, vključno z vsemi ustreznimi poslovnimi ali operativnimi dokumenti, pogodbami, dokumentacijo o politikah, revizijskimi poročili o varnosti IKT, poročili o incidentih, povezanih z IKT, ter vse informacije v zvezi s stranmi, ki jim je ključni tretji ponudnik storitev IKT oddal operativne funkcije ali dejavnosti v zunanje izvajanje.

2. Pri pošiljanju preprostega zahtevka za informacije iz odstavka 1 glavni nadzornik:

(a) navede sklic na ta člen kot pravno podlago za zahtevek;

(b) navede namen zahtevka;

(c) natančno opredeli, katere informacije se zahtevajo;

(d) določi rok, do katerega je treba predložiti informacije;

(e) obvesti predstavnika ključnega tretjega ponudnika storitev IKT, od katerega se zahtevajo informacije, da mu ni zavezan posredovati informacij, vendar v primeru prostovoljnega odgovora na zahtevek posredovane informacije ne smejo biti napačne ali zavajajoče.

3. Kadar s sklepom zahteva predložitev informacij iz odstavka 1, glavni nadzornik:

(a) navede sklic na ta člen kot pravno podlago za zahtevek;

(b) navede namen zahtevka;

(c) natančno opredeli, katere informacije se zahtevajo;

(d) določi rok, do katerega je treba predložiti informacije;

(e) navede periodične denarne kazni, določene v členu 35(6), kadar so predložene zahtevane informacije nepopolne ali če niso predložene v roku iz točke (d) tega odstavka;

(f) opozori na pravico do pritožbe zoper sklep pri odboru evropskega nadzornega organa za pritožbe ter pravico, da sklep predloži v presojo Sodišču Evropske unije (v nadaljnjem besedilu: Sodišče) v skladu s členoma 60 in 61 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

4. Predstavniki ključnih tretjih ponudnikov storitev IKT predložijo zahtevane informacije. Pooblaščeni odvetniki lahko predložijo informacije v imenu svojih strank. Ključni tretji ponudniki storitev IKT so kljub temu v celoti odgovorni, če so predložene informacije nepopolne, napačne ali zavajajoče.

5. Glavni nadzornik nemudoma pošlje kopijo odločitve o posredovanju informacij pristojnim organom finančnih subjektov, ki uporabljajo storitve zadevnih ključnih tretjih ponudnikov storitev IKT, in skupni nadzorni mreži.

Člen 38

Splošne preiskave

1. Za namene izvajanja nalog na podlagi te uredbe lahko glavni nadzornik ob pomoči skupne pregledniške ekipe iz člena 40(1) po potrebi opravi preiskave ključnih tretjih ponudnikov storitev IKT.

2. Glavni nadzornik ima pooblastila, da:

(a) preuči evidence, podatke, postopke in vse drugo gradivo, relevantno za izvajanje njegovih nalog, ne glede na vrsto nosilca podatkov, na katerem so shranjeni;

(b) izdela ali pridobi overjene kopije ali izvlečke iz takih evidenc, podatkov, dokumentiranih postopkov in kakršnega koli drugega gradiva;

(c) pozove predstavnike ključnih tretjih ponudnikov storitev IKT, naj zagotovijo ustna ali pisna pojasnila glede dejstev ali dokumentov, povezanih s predmetom in namenom preiskave, ter zabeleži njihove odgovore;

(d) opravi razgovor s katero koli drugo fizično ali pravno osebo, ki privoli v razgovor, za namen zbiranja informacij o predmetu preiskave;

(e) zahteva evidence o telefonskem in podatkovnem prometu.

3. Uradniki in druge osebe, ki jih glavni nadzornik pooblasti za namene preiskave iz odstavka 1, svoja pooblastila izvajajo ob predložitvi pisnega pooblastila, v katerem sta navedena predmet in namen preiskave.

V pooblastilu se navedejo tudi periodične denarne kazni iz člena 35(6), ki se naložijo, kadar zahtevane evidence, podatki, dokumentirani postopki ali katero koli drugo gradivo ali odgovori na vprašanja, zastavljena predstavnikom tretjega ponudnika storitev IKT, niso posredovani ali so nepopolni.

4. Predstavniki ključnih tretjih ponudnikov storitev IKT morajo privoliti v preiskave, ki jih s sklepom odredi glavni nadzornik. V sklepu se navedejo predmet in namen preiskave, periodične denarne kazni iz člena 35(6), pravna sredstva, ki so na voljo na podlagi uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010, ter opozori na pravico, da se sklep predloži v presojo Sodišču.

5. Glavni nadzornik pred začetkom preiskave pravočasno obvesti pristojne organe finančnih subjektov, ki uporabljajo storitve IKT zadevnega ključnega tretjega ponudnika storitev IKT o predvideni preiskavi in o identiteti pooblaščenih oseb.

Glavni nadzornik sporoči skupni nadzorni mreži vse informacije, posredovane na podlagi prvega pododstavka.

Člen 39

Inšpekcijski pregledi

1. Glavni nadzornik lahko za opravljanje nalog iz te uredbe ob pomoči skupnih pregledniških ekip iz člena 40(1) vstopi v vse poslovne prostore, na zemljišča ali nepremičnine tretjih ponudnikov storitev IKT, kot so sedež podjetja, operativni centri ter sekundarne lokacije, in tam izvede vse potrebne inšpekcijske preglede na kraju samem ali pa inšpekcijske preglede izvede na daljavo.

Glavni nadzornik se pri izvajanju pooblastil iz prvega pododstavka posvetuje s skupno nadzorno mrežo.

2. Uradniki in druge osebe, ki jih glavni nadzornik pooblasti za izvedbo inšpekcijskega pregleda na kraju samem, imajo pooblastila, da:

(a) vstopijo v vse take poslovne prostore, na zemljišča ali nepremičnine ter

(b) zapečatijo vse take poslovne prostore, poslovne knjige ali drugo poslovno dokumentacijo za čas trajanja inšpekcijskega pregleda in v obsegu, potrebnem za njegovo izvedbo.

Uradniki in druge osebe, ki jih pooblasti glavni nadzornik, svoja pooblastila izvajajo ob predložitvi pisnega pooblastila, v katerem so podrobno določeni predmet in namen preiskave ter periodične denarne kazni iz člena 35(6), kadar predstavniki zadevnih ključnih tretjih ponudnikov storitev IKT ne privolijo v inšpekcijski pregled.

3. Glavni nadzornik pred začetkom inšpekcijskega pregleda o njem pravočasno obvesti pristojne organe finančnih subjektov, ki uporabljajo zadevnega tretjega ponudnika storitev IKT.

4. Inšpekcijski pregledi zajemajo celoten sklop pomembnih sistemov, omrežij, naprav, informacij in podatkov na področju IKT, ki se uporabljajo za opravljanje storitev IKT finančnim subjektom ali prispevajo k njihovemu zagotavljanju.

5. Pred načrtovanim inšpekcijskim pregledom na kraju samem glavni nadzornik v razumnem roku obvesti ključne tretje ponudnike storitev IKT, razen če tega zaradi izrednih ali kriznih razmer ne more storiti ali če zaradi takega obvestila inšpekcijski pregled ali revizija ne bi bila več učinkovita.

6. Ključni tretji ponudnik storitev IKT mora privoliti v inšpekcijski pregled na kraju samem, ki ga s sklepom odredi glavni nadzornik. V sklepu se navedeta predmet in namen inšpekcijskega pregleda, določi datum, ko se bo ta začel, in navedejo periodične denarne kazni iz člena 35(6), pravna sredstva, ki so na voljo na podlagi uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010, ter opozori na pravico, da se sklep predloži v presojo Sodišču.

7. Kadar uradniki in druge osebe, ki jih pooblasti glavni nadzornik, ugotovijo, da ključni tretji ponudnik storitev IKT nasprotuje inšpekcijskemu pregledu, ki je bil odrejen na podlagi tega člena, glavni nadzornik ključnega tretjega ponudnika storitev IKT obvesti o posledicah takega nasprotovanja, vključno z možnostjo, da pristojni organi ustreznih finančnih subjektov zahtevajo, da finančni subjekti prekinejo pogodbene dogovore, sklenjene s tem ključnim tretjim ponudnikom storitev IKT.

Člen 40

Stalni nadzor

1. Glavnemu nadzorniku pri izvajanju nadzornih dejavnosti, zlasti splošnih preiskav ali inšpekcijskih pregledov, pomaga skupna pregledniška ekipa, vzpostavljena za vsakega ključnega tretjega ponudnika storitev IKT.

2. Skupno pregledniško ekipo iz odstavka 1 je sestavljajo člani osebja:

(a) evropskih nadzornih organov;

(b) ustreznih pristojnih organov, ki nadzorujejo finančne subjekte, za katere ključni tretji ponudnik storitev IKT opravlja storitve IKT;

(c) pristojnega nacionalnega organa iz člena 32(4), točka (e), na prostovoljni osnovi;

(d) enega pristojnega nacionalnega organa iz države članice, v kateri ima sedež ključni tretji ponudnik storitev IKT, na prostovoljni osnovi.

Člani skupne pregledniške ekipe morajo imeti strokovno znanje o vprašanjih s področja IKT in operativnih tveganjih. Delovanje skupne pregledniške ekipe usklajuje član osebja glavnega nadzornika, ki je imenovan za to nalogo (v nadaljnjem besedilu: koordinator glavnega nadzornika).

3. Glavni nadzornik v treh mesecih po zaključku preiskave ali inšpekcijskega pregleda in po posvetovanju z nadzorniškim forumom sprejme priporočila, ki jih naslovi na ključnega tretjega ponudnika storitev IKT na podlagi pooblastil iz člena 35.

4. Priporočila iz odstavka 3 se nemudoma sporočijo ključnemu tretjemu ponudniku storitev IKT in pristojnim organom finančnih subjektov, za katere ta opravlja storitve IKT.

Za namene izvajanja nadzornih dejavnosti lahko glavni nadzornik upošteva vsa ustrezna certificiranja, ki jih opravijo tretje strani, in notranja ali zunanja revizijska poročila tretjih strani na področju IKT, ki jih predloži ključni tretji ponudnik storitev IKT.

Člen 41

Harmonizacija pogojev, ki omogočajo izvajanje nadzornih dejavnosti

1. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih tehničnih standardov, da določijo:

(a) informacije, ki jih mora predložiti tretji ponudnik storitev IKT v zahtevku, s katerim na podlagi člena 31(11) prostovoljno zaprosi za imenovanje za ključnega ponudnika;

(b) vsebino, strukturo in obliko informacij, ki jih morajo tretji ponudniki storitev IKT predložiti, razkriti ali o njih poročati na podlagi člena 35(1), vključno s predlogo za predložitev informacij o dogovorih o podizvajanju;

(c) merila za določitev sestave skupne pregledniške ekipe, ki zagotavljajo uravnoteženo udeležbo članov osebja evropskih nadzornih organov in ustreznih pristojnih organov, njihovo imenovanje, naloge in delovne dogovore;

(d) podrobnosti ocene pristojnih organov o ukrepih, ki so jih sprejeli ključni tretji ponudniki storitev IKT na podlagi priporočil glavnega nadzornika na podlagi člena 42(3).

2. Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 17. julija 2024.

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz odstavka 1 v skladu s postopkom iz členov 10 do 14 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

Člen 42

Nadaljnje ukrepanje s strani pristojnih organov

1. V 60 koledarskih dneh po prejemu priporočil, ki jih izda glavni nadzornik na podlagi člena 31(1), točka (d), ključni tretji ponudniki storitev IKT glavnega nadzornika bodisi obvestijo, da nameravajo priporočila upoštevati, bodisi mu posredujejo utemeljeno obrazložitev, zakaj tega ne bodo storili. Glavni nadzornik te informacije takoj posreduje pristojnim organom zadevnih finančnih subjektov.

2. Glavni nadzornik javno razkrije primere, v katerih ključni tretji ponudnik storitev IKT ni obvestil glavnega nadzornika v skladu z odstavkom 1 ali kadar se šteje, da pojasnilo ključnega tretjega ponudnika storitev IKT ni zadostno. V objavljenih informacijah se razkrije identiteta ključnega tretjega ponudnika storitev IKT ter informacije o vrsti in naravi neskladnosti. Take informacije so omejene na to, kar je pomembno in sorazmerno za zagotavljanje ozaveščenosti javnosti, razen če bi taka objava povzročila nesorazmerno škodo vpletenim stranem ali resno ogrozila pravilno delovanje in integriteto finančnih trgov ali stabilnost celotnega finančnega sistema Unije ali njegovega dela.

Glavni nadzornik obvesti tretjega ponudnika storitev IKT o tem javnem razkritju.

3. Pristojni organi zadevne finančne subjekte obvestijo o tveganjih, opredeljenih v priporočilih, naslovljenih na ključne tretje ponudnike storitev IKT v skladu s členom 35(1), točka (d).

Finančni subjekti pri obvladovanju tveganja tretjih strani na področju IKT upoštevajo tveganja iz prvega pododstavka.

4. Kadar pristojni organ meni, da finančni subjekt pri obvladovanju tveganja tretje strani na področju IKT ne upošteva specifičnih tveganj, opredeljenih v priporočilih, oziroma jih ne obravnava v zadostni meri, finančni subjekt obvesti o možnosti, da bo v primeru, da ni ustreznih pogodbenih dogovorov za obravnavanje takih tveganj, v 60 koledarskih dneh sprejel odločitev v skladu z odstavkom 6.

5. Pristojni organi se lahko po prejetju poročil iz člena 35(1), točka (c), in pred sprejetjem odločitve iz odstavka 6 tega člena prostovoljno posvetujejo s pristojnimi organi, imenovanimi ali vzpostavljenimi v skladu z Direktivo (EU) 2022/2555, odgovornimi za nadzor nad bistvenim ali pomembnim subjektom, za katere velja navedena direktiva, ki je bil imenovan kot ključni tretji ponudnik storitev IKT.

6. Pristojni organi lahko kot skrajni ukrep po poslanem obvestilu oziroma posvetovanju iz odstavkov 4 in 5 tega člena v skladu s členom 50 sprejmejo odločitev, s katero od finančnih subjektov zahtevajo, da bodisi delno bodisi v celoti začasno ustavijo uporabo ali uvajanje storitve, ki jo opravlja ključni tretji ponudnik storitev IKT, dokler se ne obravnavajo tveganja, opredeljena v priporočilih, naslovljenih na ključne tretje ponudnike storitev IKT. Po potrebi lahko od finančnih subjektov zahtevajo, da delno ali v celoti prekinejo ustrezne pogodbene dogovore, sklenjene s ključnimi tretjimi ponudniki storitev IKT.

7. Kadar ključni tretji ponudnik storitev IKT na podlagi drugačnega pristopa od tistega, ki ga svetuje glavni nadzornik, zavrne potrditev priporočil in lahko tak drugačen pristop škodljivo vpliva na številne finančne subjekte ali znaten del finančnega sektorja, posamična opozorila, izdana s strani pristojnih organov, pa ne pripomorejo k doslednim pristopom, ki bi ublažili morebitno tveganje za finančno stabilnost, lahko glavni nadzornik po posvetovanju z nadzornim forumom za pristojne organe po potrebi izda nezavezujoča mnenja, ki niso javna, da bi spodbudil dosledne in usklajene nadaljnje nadzorne ukrepe.

8. Po prejemu poročil iz člena 35(1), točka (c), pristojni organi pri sprejemanju odločitve iz odstavka 6 tega člena upoštevajo vrsto in obseg tveganja, ki ga ključni tretji ponudnik storitev IKT ne obravnava, ter resnost neskladnosti, ob upoštevanju naslednjih meril:

(a) resnosti in trajanja neskladnosti;

(b) ali je neskladnost razkrila resne pomanjkljivosti v postopkih, sistemih upravljanja, obvladovanju tveganj in notranjih kontrolah ključnega tretjega ponudnika storitev IKT;

(c) ali je neskladnost omogočila, povzročila ali drugače prispevala k finančnemu kriminalu;

(d) ali je neskladnost storjena namerno ali iz malomarnosti;

(e) ali začasna prekinitev ali odpoved pogodbenih dogovorov pomeni tveganje za neprekinjeno poslovanje finančnega subjekta, ne glede na njegova prizadevanja, da se izogne motnjam pri opravljanju svojih storitev;

(f) kadar je ustrezno, mnenja, za katero se zaprosi prostovoljno v skladu z odstavkom 5 tega člena in ga izdajo pristojni organi, imenovani ali vzpostavljeni v skladu z Direktivo (EU) 2022/2555, odgovorni za nadzor bistvenega ali pomembnega subjekta, za katerega velja navedena direktiva, ki je bil imenovan kot ključni tretji ponudnik storitev IKT.

Pristojni organi finančnim subjektom odobrijo potrebno obdobje za prilagoditev pogodbenih dogovorov s ključnimi tretjimi ponudniki storitev IKT, da bi preprečili škodljive učinke na njihovo digitalno operativno odpornost ter jim omogočili uporabo izhodnih strategij in prehodnih načrtov iz člena 28.

9. Odločitev iz odstavka 6 tega člena se sporoči članom nadzornega foruma iz člena 32(4), točke (a), (b) in (c), in skupni nadzorni mreži.

Ključni tretji ponudniki storitev IKT, na katere vplivajo odločitve iz odstavka 6, v celoti sodelujejo z zadevnimi finančnimi subjekti, zlasti v okviru postopka začasne prekinitve ali odpovedi njihovih pogodbenih dogovorov.

10. Pristojni organi glavnega nadzornika redno obveščajo o pristopih in ukrepih, sprejetih pri njihovih nadzornih nalogah v zvezi s finančnimi subjekti, ter o pogodbenih dogovorih, ki jih ti sprejmejo, kadar ključni tretji ponudniki storitev IKT niso delno ali v celoti sprejeli priporočil, ki jih je nanje naslovil glavni nadzornik.

11. Glavni nadzornik lahko na zahtevo zagotovi dodatna pojasnila o izdanih priporočilih, da bi pristojne organe usmerjal pri nadaljnjih ukrepih.

Člen 43

Nadomestila za nadzor

1. Glavni nadzornik v skladu z delegiranim aktom iz odstavka 2 tega člena ključnim tretjim ponudnikom storitev IKT zaračuna nadomestila, ki v celoti pokrivajo izdatke, ki jih ima pri izvajanju nadzornih nalog v skladu s to uredbo, vključno s povračilom stroškov, ki lahko nastanejo zaradi dela, ki ga opravi skupna pregledniška ekipa iz člena 40, pa tudi stroškov svetovanja neodvisnih strokovnjakov, kot je navedeno v členu 32(4), drugi pododstavek, v zvezi z zadevami, ki spadajo v okvir neposrednih nadzornih dejavnosti.

Znesek nadomestila, ki se zaračuna ključnemu tretjemu ponudniku storitev IKT, krije vse stroške, ki nastanejo zaradi izvajanja nalog iz tega oddelka, in je sorazmeren z njegovim prometom.

2. Na Komisijo se prenese pooblastilo, da do 17. julija 2024 sprejme delegirani akt v skladu s členom 57 za dopolnitev te uredbe, v katerem določi višino nadomestil in način njihovega plačila.

Člen 44

Mednarodno sodelovanje

1. Brez poseganja v člen 36 lahko EBA, ESMA in EIOPA v skladu s členom 33 uredb (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010 sklepajo upravne dogovore z regulativnimi in nadzornimi organi tretjih držav za spodbujanje mednarodnega sodelovanja v zvezi s tveganji tretjih strani na področju IKT v različnih finančnih sektorjih, zlasti z razvojem najboljših praks za pregled praks in kontrol za obvladovanje tveganj na področju IKT, blažilnih ukrepov in odzivov na incidente.

2. Evropski nadzorni organi prek Skupnega odbora Evropskemu parlamentu, Svetu in Komisiji vsakih pet let predložijo skupno zaupno poročilo, ki povzema ugotovitve ustreznih razprav z organi tretjih držav iz odstavka 1, pri čemer je poudarek na razvoju tveganj tretjih strani na področju IKT in posledicah za finančno stabilnost, celovitost trga, zaščito vlagateljev in delovanje notranjega trga.

POGLAVJE VI

Dogovori o izmenjavi informacij

Člen 45

Dogovori o izmenjavi informacij in obveščevalnih podatkov o kibernetskih grožnjah

1. Finančni subjekti si lahko med seboj izmenjujejo informacije in obveščevalne podatke o kibernetskih grožnjah, vključno s kazalniki ogroženosti, taktikami, tehnikami in postopki, opozorili glede kibernetske varnosti in orodji za konfiguracijo, če taka izmenjava informacij in obveščevalnih podatkov:

(a) stremi k povečanju digitalne operativne odpornosti finančnih subjektov, zlasti z ozaveščanjem o kibernetskih grožnjah, k omejevanju ali oviranju zmožnosti širjenja kibernetskih groženj ter podpiranju obrambnih zmožnosti, tehnik odkrivanja groženj, blažilnih ukrepov ali faz odzivanja in okrevanja;

(b) poteka v zaupanja vrednih skupnostih finančnih subjektov;

(c) se izvaja z dogovori o izmenjavi informacij, ki ščitijo potencialno občutljivo naravo izmenjanih informacij in ki jih urejajo pravila ravnanja ob polnem spoštovanju poslovne zaupnosti, varstva osebnih podatkov v skladu z Uredbo (EU) 2016/679 in smernic o politiki konkurence.

2. Za namene odstavka 1, točka (c), dogovori o izmenjavi informacij opredeljujejo pogoje za sodelovanje in, kadar je ustrezno, določajo podrobnosti o sodelovanju javnih organov in vlogi, v kateri so lahko slednji povezani z dogovori o izmenjavi informacij, ter o sodelovanju tretjih ponudnikov storitev IKT in o operativnih elementih, vključno z uporabo namenskih informacijskih platform.

3. Finančni subjekti obvestijo pristojne organe o svojem sodelovanju pri dogovorih o izmenjavi informacij iz odstavka 1 po potrditvi njihovega članstva ali, če je ustrezno to, o prenehanju članstva, ko to začne veljati.

POGLAVJE VII

Pristojni organi

Člen 46

Pristojni organi

Brez poseganja v določbe o okviru nadzora za ključne tretje ponudnike storitev IKT iz poglavja V, oddelek II, te uredbe izpolnjevanje te uredbe zagotavljajo pristojni organi v skladu s pooblastili, podeljenimi z ustreznimi pravnimi akti, in sicer:

(a) za kreditne institucije in institucije, izvzete na podlagi Direktive 2013/36/EU, pristojni organ, imenovan v skladu s členom 4 navedene direktive, in za kreditne institucije, razvrščene kot pomembne v skladu s členom 6(4) Uredbe (EU) št. 1024/2013, ECB v skladu s pooblastili in nalogami, prenesenimi z navedeno uredbo;

(b) za plačilne institucije, vključno s plačilnimi institucijami, izvzetimi na podlagi Direktive (EU) 2015/2366, institucije za izdajo elektronskega denarja, vključno s tistimi, ki so izvzete na podlagi Direktive 2009/110/ES, in ponudnike storitev zagotavljanja informacij o računih iz člena 33(1) Direktive (EU) 2015/2366 pristojni organ, imenovan v skladu s členom 22 Direktive (EU) 2015/2366;

(c) za investicijska podjetja pristojni organ, imenovan v skladu s členom 4 Direktive (EU) 2019/2034 Evropskega parlamenta in Sveta ([38]);

(d) za ponudnike storitev v zvezi s kriptosredstvi, pooblaščene na podlagi uredbe o trgih kriptosredstev in izdajatelje žetonov, vezanih na sredstva, pristojni organ, imenovan v skladu z ustrezno določbo navedene uredbe;

(e) za centralne depotne družbe pristojni organ, imenovan v skladu s členom 11 Uredbe (EU) št. 909/2014;

(f) za centralne nasprotne stranke pristojni organ, imenovan v skladu s členom 22 Uredbe (EU) št. 648/2012;

(g) za mesta trgovanja in izvajalce storitev sporočanja podatkov pristojni organ, imenovan v skladu s členom 67 Direktive 2014/65/EU, in pristojni organ, kot je opredeljen v členu 2(1), točka 18, Uredbe (EU) št. 600/2014;

(h) za repozitorije sklenjenih poslov pristojni organ, imenovan v skladu s členom 22 Uredbe (EU) št. 648/2012;

(i) za upravitelje alternativnih investicijskih skladov pristojni organ, imenovan v skladu s členom 44 Direktive 2011/61/EU;

(j) za družbe za upravljanje pristojni organ, imenovan v skladu s členom 97 Direktive 2009/65/ES;

(k) za zavarovalnice in pozavarovalnice pristojni organ, imenovan v skladu s členom 30 Direktive 2009/138/ES;

(l) za zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj pristojni organ, imenovan v skladu s členom 12 Direktive (EU) 2016/97;

(m) za institucije za zagotavljanje poklicnega pokojninskega zavarovanja pristojni organ, imenovan v skladu s členom 47 Direktive (EU) 2016/2341;

(n) za bonitetne agencije pristojni organ, imenovan v skladu s členom 21 Uredbe (ES) št. 1060/2009;

(o) za upravljavce ključnih referenčnih vrednosti pristojni organ, imenovan v skladu s členoma 40 in 41 Uredbe (EU) 2016/1011;

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

(p) za ponudnike storitev množičnega financiranja pristojni organ, imenovan v skladu s členom 29 Uredbe (EU) 2020/1503;

(q) za repozitorije listinjenj pristojni organ, imenovan v skladu s členoma 10 in 14(1) Uredbe (EU) 2017/2402.

Člen 47

Sodelovanje s strukturami in organi, vzpostavljenimi z Direktivo (EU) 2022/2555

1. Za spodbujanje sodelovanja in omogočanje nadzornih izmenjav med pristojnimi organi, imenovanimi na podlagi te uredbe, in skupino za sodelovanje, ustanovljeno s členom 14 Direktive (EU) 2022/2555, lahko evropski nadzorni organi in pristojni organi sodelujejo pri dejavnostih skupine za sodelovanje pri vprašanjih, ki zadevajo njihove nadzorne dejavnosti v zvezi s finančnimi subjekti. Evropski nadzorni organi in pristojni organi lahko zaprosijo, da jih povabijo k sodelovanju pri dejavnostih skupine za sodelovanje pri vprašanjih v zvezi z bistvenimi ali pomembnimi subjekti, za katere velja Direktiva (EU) 2022/2555, ki so bili obenem imenovani kot ključni tretji ponudniki storitev IKT na podlagi člena 31 te uredbe.

2. Pristojni organi se lahko po potrebi posvetujejo in si izmenjajo informacije z enotnimi kontaktnimi točkami in skupinami CSIRT, imenovanimi ali vzpostavljenimi v skladu z Direktivo (EU) 2022/2555.

3. Pristojni organi lahko pristojne organe, imenovane ali vzpostavljene v skladu z Direktivo (EU) 2022/2555, po potrebi zaprosijo za vse ustrezne tehnične nasvete in sklenejo dogovore o sodelovanju, ki omogočajo vzpostavitev učinkovitih in hitrih usklajevalnih mehanizmov.

4. Z dogovori iz odstavka 3 tega člena je mogoče med drugim določiti postopke za usklajevanje nadzornih dejavnosti v zvezi z bistvenimi ali pomembnimi subjekti, za katere velja Direktiva (EU) 2022/2555, ki so bili imenovani kot ključni tretji ponudniki storitev IKT na podlagi člena 31 te uredbe, vključno z izvajanjem preiskav in inšpekcijskih pregledov na kraju samem v skladu z nacionalnim pravom ter mehanizmi za izmenjavo informacij med pristojnimi organi na podlagi te uredbe in pristojnimi organi, imenovanimi ali vzpostavljenimi v skladu z navedeno direktivo, kar vključuje dostop do informacij, ki jih zahtevajo ti organi.

Člen 48

Sodelovanje med organi

1. Pristojni organi tesno sodelujejo med seboj in po potrebi z glavnim nadzornikom.

2. Pristojni organi in glavni nadzornik si pravočasno izmenjajo vse ustrezne informacije o ključnih tretjih ponudnikih storitev IKT, ki jih potrebujejo za izvajanje svojih nalog na podlagi te uredbe, zlasti v zvezi z ugotovljenimi tveganji, pristopi in ukrepi, sprejetimi v okviru nadzornih nalog glavnega nadzornika.

Člen 49

Finančne medsektorske vaje, obveščanje in sodelovanje

1. Evropski nadzorni organi lahko prek Skupnega odbora in v sodelovanju s pristojnimi organi, organi za reševanje iz člena 3 Direktive 2014/59/EU, ECB, enotnim odborom za reševanje, kar zadeva informacije o subjektih, ki spadajo na področje uporabe Uredbe (EU) št. 806/2014, ESRB oziroma ENISA vzpostavijo mehanizme, ki omogočajo izmenjavo učinkovitih praks med finančnimi sektorji za povečanje situacijskega zavedanja in prepoznavanje skupnih kibernetskih ranljivosti in tveganj med sektorji.

Oblikujejo lahko vaje za obvladovanje kriz in izrednih razmer, ki vključujejo scenarije kibernetskih napadov, da bi razvili komunikacijske kanale in postopoma omogočili učinkovit usklajen odziv na ravni Unije v primeru večjega čezmejnega incidenta, povezanega z IKT, ali s tem povezane grožnje, ki bi imela sistemski učinek na celotni finančni sektor Unije.

Z navedenimi vajami se lahko po potrebi testira tudi odvisnost finančnega sektorja od drugih gospodarskih sektorjev.

2. Pristojni organi, evropski nadzorni organi in ECB tesno sodelujejo in si izmenjujejo informacije za izvajanje svojih nalog na podlagi členov 47 do 54. Tesno usklajujejo svoj nadzor, da bi opredelili in odpravili kršitve te uredbe, razvili in spodbujali najboljše prakse, olajšali sodelovanje, spodbujali usklajeno razlago in zagotavljali ocene med jurisdikcijami v primeru nesoglasij.

Člen 50

Upravne sankcije in popravni ukrepi

1. Pristojni organi imajo vsa pooblastila za nadzor, preiskovanje in izrekanje sankcij, potrebna za izpolnjevanje njihovih nalog na podlagi te uredbe.

2. Pooblastila iz odstavka 1 zajemajo vsaj naslednja pooblastila za:

(a) dostop do katerega koli dokumenta ali podatkov v kakršni koli obliki, za katerega pristojni organ meni, da bi lahko bil pomemben za izvajanje njegovih nalog, ter prejem ali izdelava njegove kopije;

(b) opravljanje inšpekcijskih pregledov ali preiskav na kraju samem, kar vključuje, vendar ni omejeno na:

  (i) poziv predstavnikom finančnih subjektov, naj zagotovijo ustna ali pisna pojasnila glede dejstev ali dokumentov, povezanih s predmetom in namenom preiskave, ter evidentiranje njihovih odgovorov;

  (ii) razgovor s katero koli drugo fizično ali pravno osebo, ki v to privoli, za namen zbiranja informacij o predmetu preiskave;

(c) zahtevo, da se izvedejo obnovitveni in popravni ukrepi za kršitve zahtev te uredbe.

3. Brez poseganja v pravico držav članic, da naložijo kazenske sankcije v skladu s členom 52, države članice vzpostavijo pravila, ki določajo ustrezne upravne sankcije in popravne ukrepe za kršitve te uredbe, ter zagotovijo njihovo učinkovito izvajanje.

Te sankcije in ukrepi morajo biti učinkoviti, sorazmerni in odvračilni.

4. Države članice na pristojne organe prenesejo pooblastilo, da v primeru kršitev te uredbe uporabijo vsaj naslednje upravne kazni ali popravne ukrepe:

(a) izdajo odredbo, ki od fizične ali pravne osebe zahteva, da preneha z ravnanjem, s katerim krši to uredbo, in da tega ravnanja več ne ponovi;

(b) zahtevajo začasno ali trajno prenehanje prakse ali ravnanja, za katerega pristojni organ meni, da je v nasprotju z določbami te uredbe, in preprečijo, da bi se taka praksa ali ravnanje ponovilo;

(c) sprejmejo kakršni koli ukrep, tudi denarni, za zagotovitev, da finančni subjekti še naprej izpolnjujejo zakonske zahteve;

(d) kolikor to dovoljuje nacionalno pravo, zahtevajo obstoječe evidence o podatkovnem prometu, ki jih ima telekomunikacijski operater, kadar obstaja utemeljen sum kršitve te uredbe in kadar so lahko take evidence pomembne za preiskavo kršitev te uredbe, ter

(e) izdajajo javna obvestila, vključno z javnimi izjavami, ki navajajo identiteto fizične ali pravne osebe in naravo kršitve.

5. Kadar se odstavek 2, točka (c), in odstavek 4 uporabljata za pravne osebe, države članice na pristojne organe prenesejo pooblastilo, da v skladu s pogoji iz nacionalnega prava članom upravljalnega organa in drugim posameznikom, ki so v skladu z nacionalnim pravom odgovorni za kršitev, naložijo upravne sankcije in popravne ukrepe.

6. Države članice zagotovijo, da je vsaka odločitev o naložitvi upravnih sankcij ali popravnih ukrepov, določenih v odstavku 2, točka (c), ustrezno obrazložena in da v zvezi z njo velja pravica do pritožbe.

Člen 51

Izvajanje pooblastil za nalaganje upravnih sankcij in popravnih ukrepov

1. Pristojni organi izvajajo pooblastila za nalaganje upravnih sankcij in popravnih ukrepov iz člena 50 v skladu s svojim nacionalnim pravnim okvirom, kot je ustrezno:

(a) neposredno;

(b) v sodelovanju z drugimi organi;

(c) v okviru svoje pristojnosti s prenosom pooblastil na druge organe ali

(d) z vložitvijo zahtevka pri pristojnih sodnih organih.

2. Pristojni organi pri določitvi vrste in ravni upravne kazni ali popravnega ukrepa, naloženega na podlagi člena 50, upoštevajo, v kolikšni meri je kršitev namerna ali posledica malomarnosti ter vse druge zadevne okoliščine, po potrebi tudi:

(a) pomen, resnost in trajanje kršitve;

(b) stopnjo odgovornosti fizične ali pravne osebe, ki je odgovorna za kršitev;

(c) finančno trdnost odgovorne fizične ali pravne osebe;

(d) pomen pridobljenih dobičkov ali preprečenih izgub s strani odgovorne fizične ali pravne osebe, če jih je mogoče opredeliti;

(e) izgube, ki so jih zaradi kršitve imele tretje strani, če jih je mogoče določiti;

(f) raven sodelovanja odgovorne fizične ali pravne osebe s pristojnim organom, brez poseganja v potrebo po zagotovitvi povračila pridobljenega dobička ali preprečene izgube te fizične ali pravne osebe na podlagi kršitve;

(g) prejšnje kršitve odgovorne fizične ali pravne osebe.

Člen 52

Kazenske sankcije

1. Države članice lahko sklenejo, da ne bodo določile pravil o upravnih sankcijah ali popravnih ukrepih za kršitve, za katere se v njihovem nacionalnem pravu uporabljajo kazenske sankcije.

2. Kadar države članice sklenejo določiti kazenske sankcije za kršitve te uredbe, zagotovijo, da so vzpostavljeni ustrezni ukrepi, na podlagi katerih imajo pristojni organi na voljo vsa potrebna pooblastila za sodelovanje s sodnimi organi, organi pregona ali pravosodnimi organi v njihovi jurisdikciji, da prejemajo specifične informacije, povezane s kazenskimi preiskavami ali postopki, sproženimi ob kršitvah te uredbe, in da enake informacije zagotovijo drugim pristojnim organom ter EBA, ESMA ali EIOPA, da jim omogočijo izpolnitev njihove obveznosti sodelovanja za namene te uredbe.

Člen 53

Dolžnosti uradnega obveščanja

Države članice Komisijo, ESMA, EBA in EIOPA do 17. januarja 2025 uradno obvestijo o zakonih in drugih predpisih za izvajanje tega poglavja, tudi o morebitnih ustreznih kazenskopravnih določbah. Komisijo, ESMA, EBA in EIOPA brez nepotrebnega odlašanja uradno obvestijo tudi o vseh poznejših spremembah teh zakonov in drugih predpisov.

Člen 54

Objava upravnih sankcij

1. Pristojni organi na svojih uradnih spletiščih brez nepotrebnega odlašanja objavijo vsako odločitev o naložitvi upravne sankcije, zoper katero ni pritožbe, potem ko je bil naslovnik sankcije obveščen o navedeni odločitvi.

2. V objavo iz odstavka 1 se vključijo informacije o vrsti in naravi kršitve, identiteti odgovornih oseb ter naloženih sankcij.

3. Kadar pristojni organ po presoji vsakega posameznega primera meni, da bi bila objava identitete v primeru pravnih oseb ali identitete in osebnih podatkov v primeru fizičnih oseb nesorazmerna, tudi kar zadeva tveganja v zvezi z varstvom osebnih podatkov, da bi ogrozila stabilnost finančnih trgov ali nadaljevanje tekoče kazenske preiskave ali da bi, kolikor je to mogoče ugotoviti, povzročila nesorazmerno škodo udeleženi osebi, sprejme eno od naslednjih rešitev v zvezi z odločitvijo o izreku upravne sankcije:

(a) odloži objavo, dokler ni več razlogov za neobjavo;

(b) objavo izvede na anonimni podlagi v skladu z nacionalnim pravom ali

(c) odločitve ne objavi, kadar možnosti iz točk (a) in (b) ne zadostujejo za zagotovitev odprave kakršne koli nevarnosti za stabilnost finančnih trgov ali kadar taka objava ne bi bila sorazmerna s prizanesljivostjo izrečene sankcije.

4. V primeru odločitve, da se upravna sankcija objavi na anonimni podlagi v skladu z odstavkom 3, točka (b), se lahko objava ustreznih podatkov odloži.

5. Kadar pristojni organ objavi odločitev o naložitvi upravne sankcije, zoper katero je mogoča pritožba pred ustreznimi sodnimi organi, pristojni organi na svojem uradnem spletišču nemudoma dodajo te informacije in vse poznejše povezane informacije o izidu take pritožbe. Objavijo se tudi vse sodne odločbe, s katerimi se razveljavi odločitev o naložitvi upravne sankcije.

6. Pristojni organi zagotovijo, da vsaka objava iz odstavkov 1 do 4 ostane na njihovem uradnem spletišču samo za obdobje, ki je potrebno za izvajanje tega člena. To obdobje ne sme biti daljše od petih let po objavi.

Člen 55

Poslovna skrivnost

1. Za vse zaupne informacije, prejete, izmenjane ali posredovane v skladu s to uredbo, veljajo pogoji poslovne skrivnosti iz odstavka 2.

2. Obveznost varovanja poslovne skrivnosti velja za vse osebe, ki so ali so bile zaposlene pri pristojnih organih na podlagi te uredbe ali katerem koli organu ali tržnem podjetju ali fizični ali pravni osebi, na katero so ti pristojni organi prenesli svoja pooblastila, vključno z revizorji in strokovnjaki, katerih storitve so naročili.

3. Informacije, ki so poslovna skrivnost, vključno z izmenjavo informacij med pristojnimi organi v skladu s to uredbo in pristojnimi organi, imenovanimi ali vzpostavljenimi v skladu z Direktivo (EU) 2022/2555, se ne smejo razkriti nobeni drugi osebi ali organu, razen na podlagi določb prava Unije ali nacionalnega prava.

4. Vse informacije, ki si jih pristojni organi izmenjajo na podlagi te uredbe in ki zadevajo poslovne ali operativne razmere in druge gospodarske ali osebne zadeve, se štejejo za zaupne in zanje veljajo zahteve o varovanju poslovne skrivnosti, razen kadar pristojni organ v času posredovanja teh informacij navede, da se lahko razkrijejo, ali kadar je tako razkritje potrebno v sodnih postopkih.

Člen 56

Varstvo podatkov

1. Evropski nadzorni organi in pristojni organi lahko obdelujejo osebne podatke le, kadar je to potrebno za izpolnjevanje njihovih obveznosti in nalog na podlagi te uredbe, zlasti za preiskave, inšpekcijske preglede, zahteve za informacije, komunikacijo, objavo, evalvacija, preverjanje, ocenjevanje in pripravo načrtov nadzora. Osebni podatki se obdelujejo v skladu z Uredbo (EU) 2016/679 ali Uredbo (EU) 2018/1725, odvisno od tega, katera se uporablja.

2. Kadar v drugih sektorskih aktih ni določeno drugače, se osebni podatki iz odstavka 1 hranijo do izpolnitve zadevnih nadzornih nalog in v vsakem primeru največ 15 let, razen v primeru še nekončanih sodnih postopkov, zaradi katerih je treba take podatke še naprej hraniti.

POGLAVJE VIII

Delegirani akti

Člen 57

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejetje delegiranih aktov iz členov 31(6) in 43(2) se prenese na Komisijo za obdobje petih let od 17. januarja 2024. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.

3. Prenos pooblastila iz členov 31(6) in 43(2) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi členov 31(6) in 43(2), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku treh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za tri mesece.

POGLAVJE IX

Prehodne in končne določbe

Oddelek I

Člen 58

Klavzula o pregledu

1. Komisija do 17. januarja 2028 po posvetovanju z evropskimi nadzornimi organi in ESRB po potrebi opravi pregled ter Evropskemu parlamentu in Svetu predloži poročilo ter mu po potrebi priloži zakonodajni predlog. Pregled vključuje najmanj naslednje:

(a) merila za imenovanje ključnih tretjih ponudnikov storitev IKT v skladu s členom 31(2);

(b) prostovoljnost obveščanja o pomembnih kibernetskih grožnjah iz člena 19;

(c) ureditev iz člena 31(12) in pooblastila glavnega nadzornika iz člena 35(1), točka (d), točka (iv), prva alinea, da se oceni učinkovitost navedenih določb pri zagotavljanju učinkovitega nadzora nad ključnimi tretjimi ponudniki storitev IKT s sedežem v tretji državi in potreba po ustanovitvi odvisnega podjetja v Uniji.

Za namene prvega pododstavka te točke pregled vključuje analizo ureditve iz člena 31(12), vključno s pogoji dostopa finančnih subjektov Unije do storitev iz tretjih držav in razpoložljivostjo takih storitev na trgu Unije, ter upošteva nadaljnji razvoj na trgih za storitve, ki jih zajema ta uredba, praktične izkušnje finančnih subjektov in finančnih nadzornikov v zvezi z uporabo in nadzorom te ureditve ter vse relevantne regulativne in nadzorne spremembe na mednarodni ravni;

(d) ustreznost vključitve finančnih subjektov iz člena 2(3), točka (e), ki uporabljajo avtomatizirane prodajne sisteme, v področje uporabe te uredbe glede na prihodnji razvoj trga v zvezi z uporabo takih sistemov;

(e) delovanje in uspešnost skupne nadzorne mreže pri podpiranju doslednosti nadzora in učinkovitosti izmenjave informacij znotraj okvira nadzora.

2. Komisija v okviru pregleda Direktive (EU) 2015/2366 oceni potrebo po večji kibernetski odpornosti plačilnih sistemov in dejavnosti obdelave plačil ter ustreznost razširitve področja uporabe te uredbe na upravljavce plačilnih sistemov in subjekte, vključene v dejavnosti obdelave plačil. Ob upoštevanju te ocene Komisija v okviru pregleda Direktive (EU) 2015/2366 Evropskemu parlamentu in Svetu predloži poročilo najpozneje 17. julija 2023.

Komisija lahko na podlagi tega poročila o pregledu in po posvetovanju z evropskimi nadzornimi organi, ECB in ESRB po potrebi in kot del zakonodajnega predloga, ki ga lahko sprejme na podlagi člena 108, drugi odstavek, Direktive (EU) 2015/2366, predloži predlog za zagotovitev, da so vsi upravljavci plačilnih sistemov in subjekti, vključeni v dejavnosti obdelave plačil, pod ustreznim nadzorom, pri čemer se upošteva obstoječi nadzor, ki ga izvaja centralna banka.

3. Komisija do 17. januarja 2026 po posvetovanju z evropskimi nadzornimi organi in Odborom evropskih organov za nadzor revizorjev opravi pregled ter Evropskemu parlamentu in Svetu predloži poročilo, po potrebi skupaj z zakonodajnim predlogom, o ustreznosti strožjih zahtev za zakonite revizorje in revizijska podjetja glede digitalne operativne odpornosti, in sicer z vključitvijo zakonitih revizorjev in revizijskih podjetij v področje uporabe te uredbe ali s spremembami Direktive 2006/43/ES Evropskega parlamenta in Sveta ([39]).

Oddelek II

Spremembe

Člen 59

Spremembe Uredbe (ES) št. 1060/2009

Uredba (ES) št. 1060/2009 se spremeni:

(1) v Prilogi I, oddelek A, točka 4, se prvi pododstavek nadomesti z naslednjim:

„Bonitetna agencija mora imeti ustrezne upravne in računovodske postopke, mehanizme notranjih kontrol, učinkovite postopke za ocenjevanje tveganj ter učinkovite kontrolne in zaščitne ukrepe za upravljanje sistemov IKT v skladu z Uredbo (EU) 2022/2554 Evropskega parlamenta in Sveta (*).

_____

(*) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).“;

(2) v Prilogi III se točka 12 nadomesti z naslednjim:

„12. Bonitetna agencija prekrši člen 6(2) v povezavi s točko 4 oddelka A Priloge I, če nima ustreznih upravnih ali računovodskih postopkov, mehanizmov notranjih kontrol, učinkovitih postopkov za ocenjevanje tveganj ali učinkovitih kontrolnih ali zaščitnih ukrepov za upravljanje sistemov IKT v skladu z Uredbo (EU) 2022/2554 ali če ne izvaja ali ohranja postopkov odločanja ali organizacijskih struktur kot se zahteva z navedeno točko.“.

Člen 60

Spremembe Uredbe (EU) št. 648/2012

Uredba (EU) št. 648/2012 se spremeni:

(1) člen 26 se spremeni:

(a) odstavek 3 se nadomesti z naslednjim:

„3. CNS vzdržuje in upravlja organizacijsko strukturo, ki zagotavlja neprekinjenost in urejeno delovanje pri opravljanju njenih storitev in dejavnosti. Uporablja ustrezne in sorazmerne sisteme, vire in postopke, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2022/2554 Evropskega parlamenta in Sveta (*).

_____

(*) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).“;

([39]) Direktiva 2006/43/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o obveznih revizijah za letne in konsolidirane računovodske izkaze, spremembi direktiv Sveta 78/660/EGS in 83/349/EGS ter razveljavitvi Direktive Sveta 84/253/EGS (UL L 157, 9.6.2006, str. 87).

(b) odstavek 6 se črta;

(2) člen 34 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. CNS vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, ki vključuje politiko neprekinjenega poslovanja ter načrte odzivanja in okrevanja IKT, vzpostavljene in izvajane v skladu z Uredbo (EU) 2022/2554, katerih cilj je zagotoviti ohranjanje njenih funkcij, pravočasno obnovitev delovanja in izpolnitev obveznosti CNS.“;

(b) v odstavku 3 se prvi pododstavek nadomesti z naslednjim:

„3. Da se zagotovi dosledna uporaba tega člena, ESMA po posvetovanju s članicami ESCB pripravi osnutke regulativnih tehničnih standardov, ki določajo najmanjši obseg vsebine in minimalne zahteve za politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, razen za politiko neprekinjenega poslovanja na področju IKT in načrte ponovne vzpostavitve delovanja IKT.“;

(3) v členu 56(3) se prvi pododstavek nadomesti z naslednjim:

„3. Da se zagotovi dosledna uporaba tega člena, ESMA pripravi osnutke regulativnih tehničnih standardov, ki določajo podrobnosti v zvezi z vlogo za registracijo iz odstavka 1, razen za zahteve, povezane z obvladovanjem tveganj na področju IKT.“;

(4) v členu 79 se odstavka 1 in 2 nadomestita z naslednjim:

„1. Repozitorij sklenjenih poslov identificira vire operativnega tveganja in jih zmanjša na najnižjo raven tudi z razvojem ustreznih sistemov, kontrol in postopkov, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2022/2554.

2. Repozitorij sklenjenih poslov vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, vključno s politiko neprekinjenega poslovanja na področju IKT ter načrtom odzivanja in okrevanja IKT, vzpostavljenima v skladu z Uredbo (EU) 2022/2554, katerih cilj je zagotoviti ohranjanje njegovih funkcij, pravočasno obnovitev delovanja in izpolnitev obveznosti repozitorija sklenjenih poslov.“;

(5) v členu 80 se črta odstavek 1;

(6) Priloga I, oddelek II, se spremeni:

(a) točki (a) in (b) se nadomestita z naslednjim:

„(a) repozitorij sklenjenih poslov krši člen 79(1), če ne identificira virov operativnega tveganja in jih z razvojem ustreznih sistemov, kontrol in postopkov, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2022/2554, ne zmanjša na najnižjo možno raven;

(b) repozitorij sklenjenih poslov krši člen 79(2), če ne vzpostavi, izvaja ali vzdržuje ustrezne politike neprekinjenega poslovanja in načrta za vnovično vzpostavitev delovanja, vzpostavljenih v skladu z Uredbo (EU) 2022/2554, katerih cilj je zagotoviti ohranjanje funkcij, pravočasno obnovitev delovanja in izpolnitev obveznosti repozitorija sklenjenih poslov;“;

(b) točka (c) se črta;

(7) Priloga III se spremeni:

(a) oddelek II se spremeni:

(i) točka (c) se nadomesti z naslednjim:

„(c) CNS stopnje 2 krši člen 26(3), če ne ohranja ali uporablja organizacijske strukture, ki zagotavlja stalno in urejeno delovanje v zvezi z opravljanjem njenih storitev in dejavnosti ali ne uporabi ustreznih in sorazmernih sistemov, sredstev ali postopkov, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2022/2554;“;

(ii) točka (f) se črta;

(b) v oddelku III se točka (a) nadomesti z naslednjim:

„(a) CNS stopnje 2 krši člen 34(1), če ne sprejme, uveljavi ali vzdržuje ustrezne politike neprekinjenega poslovanja in načrta ponovne vzpostavitve delovanja, vzpostavljenih v skladu z Uredbo(EU) 2022/2554, s katerima zagotovi ohranitev delovanja svojih funkcij, pravočasno ponovno vzpostavitev delovanja in izpolnitev svojih obveznosti, ki v primeru motenj zagotovi najmanj ponovno vzpostavitev vseh transakcij, s čimer CNS omogoči zanesljivo nadaljnje delovanje in dokončanje poravnave na načrtovani datum;".

Člen 61

Spremembe Uredbe (EU) št. 909/2014

Člen 45 Uredbe (EU) št. 909/2014 se spremeni:

(1) odstavek 1 se nadomesti z naslednjim:

„1. CDD identificira notranje in zunanje vire operativnega tveganja in zmanjša njihov vpliv tudi z uporabo ustreznih orodij, postopkov in politik IKT, vzpostavljenih in upravljanih v skladu z Uredbo (EU) 2022/2554 Evropskega parlamenta in Sveta (*), ter z drugimi pomembnimi ustreznimi orodji, kontrolami in postopki za druge vrste operativnega tveganja, med drugim za vse sisteme poravnave vrednostnih papirjev, ki jih upravlja.

_____

(*) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).";

(2) odstavek 2 se črta;

(3) odstavka 3 in 4 se nadomestita z naslednjim:

„3. CDD za storitve, ki jih opravlja, in vse sisteme poravnave vrednostnih papirjev, ki jih upravlja, vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt za sanacijo po nesreči, vključno s politiko neprekinjenega poslovanja ter načrti odzivanja in okrevanja IKT, vzpostavljenimi v skladu z Uredbo (EU) 2022/2554, da v primeru dogodkov, za katere obstaja znatna nevarnost, da bodo povzročili motnje pri poslovanju, zagotovi ohranitev svojih storitev, pravočasno ponovno vzpostavitev poslovanja in izpolnjevanje svojih obveznosti.

4. Načrt iz odstavka 3 ob motnji poskrbi za obnovitev vseh poslov in pozicij udeležencev, da lahko udeleženci CDD še naprej poslujejo zanesljivo in poravnavo zaključijo na načrtovani datum, in sicer to omogoči tudi z zagotavljanjem, da lahko začnejo kritični sistemi informacijske tehnologije po motnji znova delovati, kot je določeno v členu 12(5) in (7) Uredbe (EU) 2022/2554.";

(4) odstavek 6 se nadomesti z naslednjim:

„6. CDD identificira, spremlja in obvladuje tveganja, ki jih za njeno poslovanje morda pomenijo ključni udeleženci v sistemih poravnave vrednostnih papirjev, ki jih upravlja, ter izvajalci javnih in drugih storitev in druge CDD ali druge tržne infrastrukture. Pristojnim in zadevnim organom na zahtevo zagotovi informacije o vsakem takem identificiranem tveganju. Hkrati pristojni organ in zadevne organe brez odlašanja obvesti o vseh operativnih incidentih, ki so posledica takih tveganj, razen o incidentih, povezanih s tveganjem na področju IKT.";

(5) v odstavku 7 se prvi pododstavek nadomesti z naslednjim:

„7. ESMA v tesnem sodelovanju s članicami ESCB pripravi osnutke regulativnih tehničnih standardov, da se določijo operativna tveganja iz odstavkov 1 in 6, razen tveganja na področju IKT, ter metode za testiranje, obravnavo ali zmanjšanje teh tveganj, vključno s politikami neprekinjenega poslovanja in načrti ponovne vzpostavitve delovanja iz odstavkov 3 in 4 ter metodami za njihovo oceno.".

Člen 62

Spremembe Uredbe (EU) št. 600/2014

Uredba (EU) št. 600/2014 se spremeni:

(1) člen 27g se spremeni:

(a) odstavek 4 se nadomesti z naslednjim:

„4. APA izpolnjuje zahteve glede varnosti omrežnih in informacijskih sistemov iz Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta (*).

(*) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).“;

(b) v odstavku 8 se točka (c) nadomesti z naslednjim:

„(c) konkretne organizacijske zahteve iz odstavkov 3 in 5.“;

(2) člen 27h se spremeni:

(a) odstavek 5 se nadomesti z naslednjim:

„5. CTP izpolnjuje zahteve glede varnosti omrežnih in informacijskih sistemov iz Uredbe (EU) 2022/2554.“;

(b) v odstavku 8 se točka (e) nadomesti z naslednjim:

„(e) konkretne organizacijske zahteve iz odstavka 4.“;

(3) člen 27i se spremeni:

(a) odstavek 3 se nadomesti z naslednjim:

„3. ARM izpolnjuje zahteve glede varnosti omrežnih in informacijskih sistemov iz Uredbe (EU) 2022/2554.“;

(b) v odstavku 5 se točka (b) nadomesti z naslednjim:

„(b) konkretne organizacijske zahteve iz odstavkov 2 in 4.“.

Člen 63

Sprememba Uredbe (EU) 2016/1011

V členu 6 Uredbe (EU) 2016/1011 se doda naslednji odstavek:

„6. Upravljavec ima za ključne referenčne vrednosti ustrezne upravne in računovodske postopke, mehanizme notranjih kontrol, učinkovite postopke za ocenjevanje tveganj ter učinkovite kontrolne in zaščitne ukrepe za upravljanje sistemov IKT v skladu z Uredbo (EU) 2022/2554 Evropskega parlamenta in Sveta (*).

(*) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).“.

Člen 64

Začetek veljavnosti in uporaba

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uporablja se od 17. januarja 2025.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Strasbourgu, 14. decembra 2022

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	M. BEK