2024/1774

25.6.2024.

KOMISIJAS DELEĢĒTĀ REGULA (ES) 2024/1774

(2024. gada 13. marts),

ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem, kuri nosaka IKT riska pārvaldības rīkus, metodes, procesus un politiku, un vienkāršoto IKT riska pārvaldības sistēmu

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 ([1]), un jo īpaši tās 15. panta ceturto daļu un 16. panta 3. punkta ceturto daļu,

tā kā:

(1) Regula (ES) 2022/2554 attiecas uz ļoti daudzveidīgu tādu finanšu vienību klāstu, kas atšķiras pēc to lieluma, struktūras, iekšējās organizācijas un to darbību veida un sarežģītības un kam tādējādi ir palielināti vai samazināti sarežģītības vai risku elementi. Lai nodrošinātu, ka šī daudzveidība tiek pienācīgi ņemta vērā, jebkurām prasībām attiecībā uz IKT drošības politiku, procedūrām, protokoliem un rīkiem un attiecībā uz vienkāršotu IKT riska pārvaldības sistēmu vajadzētu būt samērīgām ar šo finanšu vienību lielumu, struktūru, iekšējo organizāciju, veidu un sarežģītību un atbilstošajiem riskiem.

(2) Tā paša iemesla dēļ finanšu vienībām, uz kurām attiecas Regula (ES) 2022/2554, vajadzētu būt noteiktam elastīgumam attiecībā uz to, kādā veidā tās izpilda prasības saistībā ar IKT drošības politiku, procedūrām, protokoliem un rīkiem un jebkādu vienkāršotu IKT riska pārvaldības sistēmu. Jau minētā iemesla dēļ būtu jāļauj finanšu vienībām izmantot dokumentāciju, kas tām jau ir, lai izpildītu dokumentācijas prasības, kas izriet no minētajām prasībām. No tā izriet, ka īpašas IKT drošības politikas izstrāde, dokumentēšana un īstenošana būtu jāpieprasa tikai attiecībā uz konkrētiem būtiskiem elementiem, cita starpā ņemot vērā nozarē vadošo praksi un standartus. Turklāt, lai aptvertu īpašus tehniskos īstenošanas aspektus, ir jāizstrādā, jādokumentē un jāīsteno IKT drošības procedūras nolūkā aptvert īpašus tehniskus īstenošanas aspektus, tajā skaitā jaudas un veiktspējas pārvaldību, ievainojamības un ielāpu pārvaldību, datu un sistēmu drošību un reģistrēšanu žurnālā.

(3) Lai nodrošinātu šīs regulas II sadaļas I nodaļā minētās IKT drošības politikas, procedūru, protokolu un rīku pareizu īstenošanu laika gaitā, ir svarīgi, lai finanšu vienības pareizi sadalītu un uzturētu spēkā uzdevumus un atbildību, kas saistīta ar IKT drošību, un lai tās noteiktu sekas, kas rodas, ja netiek ievērota IKT drošības politika vai procedūras.

(4) Lai ierobežotu interešu konfliktu risku, finanšu vienībām, sadalot IKT uzdevumus un atbildību, būtu jānodrošina pienākumu nošķiršana.

(5) Lai nodrošinātu elastīgumu un vienkāršotu finanšu vienību kontroles sistēmu, nebūtu jāprasa, lai finanšu vienības izstrādā īpašus noteikumus par sekām, kas rodas, ja neievēro šīs regulas II sadaļas I nodaļā minēto IKT drošības politiku, procedūras un protokolus, ja šādi noteikumi jau ir izklāstīti citā politikā vai procedūrā.

([1]) OV L 333, 27.12.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) Dinamiskā vidē, kur IKT riski pastāvīgi attīstās, ir svarīgi, lai finanšu vienības izstrādātu savu IKT politikas kopumu, kas balstīts uz paraugpraksi un attiecīgā gadījumā uz standartiem, kuri noteikti Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([2]) 2. panta 1. punktā. Tam būtu jāļauj šīs regulas II sadaļā minētajām finanšu vienībām vienmēr būt informētām un sagatavotām vidē, kas ir mainīga.

(7) Lai nodrošinātu to digitālās darbības noturību, šīs regulas II sadaļā minētajām finanšu vienībām savas IKT drošības politikas, procedūru, protokolu un rīku ietvaros būtu jāizstrādā un jāīsteno IKT aktīvu pārvaldības politika, jaudas un veiktspējas pārvaldības procedūras, kā arī politika un procedūras attiecībā uz IKT darbībām. Minētā politika un procedūras ir nepieciešamas, lai nodrošinātu IKT aktīvu statusu visā to aprites ciklā, tā, lai šie aktīvi tiktu izmantoti un uzturēti lietpratīgi (IKT aktīvu pārvaldība). Minētajai politikai un procedūrām būtu arī jānodrošina IKT sistēmu darbības optimizācija un tas, ka IKT sistēmu un jaudas veiktspēja atbilst iedibinātiem uzņēmējdarbības un informācijas drošības mērķiem (jaudas un veiktspējas pārvaldība). Visbeidzot, minētajai politikai un procedūrām būtu jānodrošina efektīva un raita IKT sistēmu ikdienas pārvaldība un darbība (IKT darbības), tādējādi mazinot datu konfidencialitātes, integritātes un pieejamības zaudēšanas risku. Tādējādi minētā politika un procedūras ir nepieciešamas, lai nodrošinātu tīklu drošību, sniegtu pietiekamu aizsardzību pret ielaušanos sistēmā un datu ļaunprātīgu izmantošanu un saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti.

(8) Lai nodrošinātu mantoto IKT sistēmu riska pienācīgu pārvaldību, finanšu vienībām būtu jāreģistrē un jāuzrauga trešo personu, kas sniedz IKT atbalsta pakalpojumus, beigu datumi. Ņemot vērā datu konfidencialitātes, integritātes un pieejamības zaudēšanas iespējamo ietekmi, finanšu vienībām, reģistrējot un uzraugot minētos beigu datumus, būtu jāpievērš īpaša uzmanība tiem IKT aktīviem vai sistēmām, kas ir kritiski svarīgi uzņēmuma darbībai.

(9) Kriptogrāfiskās kontroles var nodrošināt datu pieejamību, autentiskumu, integritāti un konfidencialitāti. Tāpēc šīs regulas II sadaļā minētajām finanšu vienībām būtu jāidentificē un jāīsteno šādas kontroles, izmantojot uz risku balstītu pieeju. Šajā nolūkā finanšu vienībām būtu jāšifrē attiecīgie dati, kad tie tiek glabāti, pārsūtīti vai, ja nepieciešams, lietoti, pamatojoties uz divējāda procesa, proti, datu klasifikācijas un visaptveroša IKT riska novērtējuma, rezultātiem. Ņemot vērā lietošanā esošu datu šifrēšanas sarežģītību, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāšifrē lietošanā esoši dati tikai tad, ja tas būtu atbilstoši, ņemot vērā IKT riska novērtējuma rezultātus. Tomēr gadījumos, kad lietošanā esošu datu šifrēšana nav iespējama vai ir pārāk sarežģīta, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāspēj aizsargāt attiecīgo datu konfidencialitāti, integritāti un pieejamību, īstenojot citus IKT drošības pasākumus. Ņemot vērā tehnoloģiju straujo attīstību kriptogrāfijas metožu jomā, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāseko līdzi attiecīgajām norisēm kriptoanalīzes jomā un jāņem vērā paraugprakse un standarti. Tādējādi šīs regulas II sadaļā minētajām finanšu vienībām būtu jāizmanto elastīga pieeja, kas balstīta uz riska mazināšanu un uzraudzību, lai pārvaldītu kriptogrāfisko apdraudējumu – ieskaitot apdraudējumus, ko rada sasniegumi kvantu jomā, – dinamisko vidi.

(10) IKT darbību drošībai un darbības politikai, procedūrām, protokoliem un rīkiem ir būtiska nozīme, lai nodrošinātu datu konfidencialitāti, integritāti un pieejamību. Viens no izšķirīgajiem faktoriem ir IKT ražošanas vides nošķiršana no vides, kur tiek izstrādātas un testētas IKT sistēmas, un no citām neražošanas vidēm. Šai nošķiršanai vajadzētu būt svarīgam IKT drošības pasākumam, kas aizsargā pret neparedzētu un neatļautu piekļuvi datiem, to pārveidošanu un dzēšanu ražošanas vidē, kā rezultātā var rasties būtiski šīs regulas II sadaļā minēto finanšu vienību uzņēmējdarbības traucējumi. Tomēr, ņemot vērā pašreizējo IKT sistēmu izstrādes praksi, izņēmuma apstākļos būtu jāļauj finanšu vienībām veikt testēšanu ražošanas vidē ar nosacījumu, ka tās pamato šādu testēšanu un saņem vajadzīgo apstiprinājumu.

([2]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp., ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Ņemot vērā strauji mainīgo IKT vidi, IKT ievainojamību un kiberdraudus, ir vajadzīga proaktīva un visaptveroša pieeja IKT ievainojamības identificēšanai, izvērtēšanai un risināšanai. Bez šādas pieejas finanšu vienības, to klienti, lietotāji vai darījumu partneri var būt būtiski pakļauti riskiem, un tas, savukārt, apdraudētu to digitālās darbības noturību, to tīklu drošību un datu, kas IKT drošības politikai un procedūrām būtu jāaizsargā, pieejamību, autentiskumu, integritāti un konfidencialitāti. Tāpēc šīs regulas II sadaļā minētajām finanšu vienībām būtu jāidentificē un jānovērš to IKT vides ievainojamība, un gan finanšu vienībām, gan trešām personām, kas tām sniedz IKT pakalpojumus, būtu jāīsteno saskanīga, pārredzama un atbildīga ievainojamības pārvaldības sistēma. Tā paša iemesla dēļ finanšu vienībām būtu jāuzrauga IKT ievainojamība, izmantojot uzticamus resursus un automatizētus rīkus, pārliecinoties, ka trešās personas, kas sniedz IKT pakalpojumus, nodrošina ātru rīcību saistībā ar ievainojamību sniegtajos IKT pakalpojumos.

(12) Ielāpu pārvaldībai vajadzētu būt būtiskai daļai no šīs IKT drošības politikas un procedūrām, kurām, veicot testēšanu un izvēršanu kontrolētā vidē, ir jārisina identificētā ievainojamība un jānovērš traucējumi, ko rada ielāpu instalēšana.

(13) Lai nodrošinātu, ka iespējamie drošības apdraudējumi, kas var ietekmēt finanšu vienību un tās ieinteresētās personas, tiek laikus un pārredzami paziņoti, finanšu vienībām būtu jāievieš procedūras atbildīgai IKT ievainojamības paziņošanai klientiem, darījumu partneriem un sabiedrībai. Šādu procedūru ieviešanā finanšu vienībām būtu jāņem vērā dažādi faktori, tajā skaitā ievainojamības būtiskums, šādas ievainojamības potenciālā ietekme uz ieinteresētajām personām un risinājuma vai mazināšanas pasākumu gatavība.

(14) Lai varētu piešķirt lietotāju piekļuves tiesības, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāievieš stingri pasākumi, lai pārbaudītu to personu un sistēmu unikālo identifikāciju, kuras piekļūs finanšu vienības informācijai. Pretējā gadījumā finanšu vienības saskartos ar potenciālu neatļautu piekļuvi, datu aizsardzības pārkāpumiem un krāpnieciskām darbībām, tādējādi apdraudot sensitīvu finanšu datu konfidencialitāti, integritāti un pieejamību. Lai gan izņēmuma kārtā apstākļos, ko nosaka finanšu vienības, būtu jāatļauj vispārīgu vai kopīgu kontu izmantošana, finanšu vienībām būtu jānodrošina, ka tiek saglabāta pārskatatbildība par darbībām, kas tiek veiktas ar šo kontu starpniecību. Ja nebūtu šā aizsardzības pasākuma, potenciālie ļaunprātīgie lietotāji varētu traucēt izmeklēšanas un korektīviem pasākumiem, kā rezultātā finanšu vienības kļūtu neaizsargātas pret neatklātām ļaunprātīgām darbībām vai sodiem par neatbilstību.

(15) Lai pārvaldītu IKT vides straujo attīstību, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāīsteno stingra IKT projektu pārvaldības politika un procedūras nolūkā saglabāt datu pieejamību, autentiskumu, integritāti un konfidencialitāti. Minētajā IKT projektu pārvaldības politikā un procedūrās būtu jānosaka tie elementi, kas ir nepieciešami, lai veiksmīgi pārvaldītu IKT projektus, tajā skaitā izmaiņas finanšu vienības IKT sistēmās, šo sistēmu iegādi, uzturēšanu un attīstību, neatkarīgi no finanšu vienības izvēlētās IKT projektu pārvaldības metodikas. Šīs politikas un procedūru kontekstā finanšu vienībām būtu jāizmanto testēšanas prakse un metodes, kas ir atbilstošas to vajadzībām, vienlaikus ievērojot uz risku balstītu pieeju un nodrošinot, ka tiek uzturēta droša, uzticama un noturīga IKT vide. Lai garantētu IKT projekta drošu īstenošanu, finanšu vienībām būtu jānodrošina, ka personāls no īpašām uzņēmējdarbības nozarēm vai funkcijām, ko ietekmē attiecīgais IKT projekts, var sniegt nepieciešamo informāciju un zinātību. Lai nodrošinātu efektīvu pārraudzību, būtu jāiesniedz vadības struktūrai ziņojumi par IKT projektiem, jo īpaši tiem, kas ietekmē kritiski svarīgas vai svarīgas funkcijas, un par to saistītajiem riskiem. Finanšu vienībām sistemātisko un pastāvīgo pārskatu un ziņojumu biežums un detalizācija būtu jāpielāgo attiecīgo IKT projektu svarīgumam un lielumam.

(16) Ir jānodrošina, ka programmatūras pakotnes, ko šīs regulas II sadaļā minētās finanšu vienības iegādājas un izstrādā, tiek efektīvi un droši integrētas esošajā IKT vidē saskaņā ar iedibinātiem uzņēmējdarbības un informācijas drošības mērķiem. Tāpēc finanšu vienībām būtu regulāri jāizvērtē šādas programmatūras pakotnes. Šajā nolūkā un lai identificētu ievainojamību un potenciālās drošības plaisas gan programmatūras pakotnēs, gan plašākās IKT sistēmās, finanšu vienībām būtu jāveic IKT drošības testēšana. Lai novērtētu programmatūras integritāti un nodrošinātu, ka šīs programmatūras izmantošana nerada IKT drošības riskus, finanšu vienībām, izmantojot gan statiskās, gan dinamiskās testēšanas metodes, būtu arī jāpārskata iegādātās programmatūras pirmkodi, tajā skaitā, ja iespējams, arī tās programmatūras pirmkodi, kuru nodrošina trešās personas, kas sniedz IKT pakalpojumus.

(17) Izmaiņas neatkarīgi no to apjoma ir saistītas ar raksturīgiem riskiem un var radīt ievērojamus datu konfidencialitātes, integritātes un pieejamības zaudēšanas riskus, un tādējādi var izraisīt nopietnus uzņēmējdarbības traucējumus. Lai pasargātu finanšu vienības no varbūtējas IKT ievainojamības un nepilnībām, kuru dēļ tās var būt pakļautas ievērojamiem riskiem, ir vajadzīgs stings verifikācijas process, lai apstiprinātu, ka visas izmaiņas atbilst nepieciešamajām IKT drošības prasībām. Tāpēc šīs regulas II sadaļā minētajām finanšu vienībām kā būtisks to IKT drošības politikas un procedūru elements būtu jāievieš pārdomāta IKT izmaiņu pārvaldības politika un procedūras. Lai uzturētu IKT izmaiņu pārvaldības procesa objektivitāti un efektivitāti, novērstu interešu konfliktus un nodrošinātu, ka IKT izmaiņas tiek izvērtētas objektīvi, ir jānošķir funkcijas, kas atbild par šo izmaiņu apstiprināšanu, no funkcijām, kas pieprasa un īsteno šīs izmaiņas. Lai panāktu efektīvu pāreju, kontrolētu IKT izmaiņu ieviešanu un to, ka traucējumi IKT sistēmu darbībā tiek samazināti līdz minimumam, finanšu vienībām būtu jāpiešķir skaidri uzdevumi un atbildība, lai nodrošinātu, ka IKT izmaiņas ir plānotas, tiek pienācīgi testētas un ka tiek nodrošināta kvalitāte. Lai nodrošinātu, ka IKT sistēmas turpina efektīvi darboties, un radītu drošības tīklu finanšu vienībām, finanšu vienībām būtu arī jāizstrādā un jāīsteno darbības nepārtrauktības procedūras. Finanšu vienībām būtu skaidri jāidentificē šīs darbības nepārtrauktības procedūras un jāsadala atbildība, lai nodrošinātu ātru un efektīvu reaģēšanu neveiksmīgu IKT izmaiņu gadījumā.

(18) Lai atklātu, pārvaldītu ar IKT saistītus incidentus un ziņotu par tiem, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāizstrādā ar IKT saistītu incidentu politika, kas ietver ar IKT saistītu incidentu pārvaldības procesa elementus. Šajā nolūkā finanšu vienībām būtu jāidentificē visas attiecīgās kontaktpersonas organizācijas iekšienē un ārpus tās, kas var veicināt dažādo šā procesa posmu pareizu koordināciju un īstenošanu. Lai optimizētu ar IKT saistītu incidentu atklāšanu un reaģēšanu uz tiem un identificētu šo incidentu tendences, kas ir vērtīgs informācijas avots, kurš ļauj finanšu vienībām efektīvi apzināt un risināt cēloņus un problēmas, finanšu vienībām jo īpaši būtu sīki jāanalizē ar IKT saistītie incidenti, ko tās uzskata par nozīmīgākajiem, cita starpā arī tāpēc, ka tie regulāri atkārtojas.

(19) Lai garantētu anomālu darbību agrīnu un efektīvu atklāšanu, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāvāc, jāuzrauga un jāanalizē dažādie informācijas avoti un jāsadala saistītie uzdevumi un atbildība. Attiecībā uz iekšējiem informācijas avotiem ļoti svarīgs avots ir žurnāli, taču finanšu vienībām nebūtu jāpaļaujas tikai uz žurnāliem. Finanšu vienībām būtu jāņem vērā plašāka informācija, lai iekļautu to, ko paziņo citas iekšējās funkcijas, jo šīs funkcijas bieži ir vērtīgs svarīgas informācijas avots. Tā paša iemesla dēļ finanšu vienībām būtu jāanalizē un jāuzrauga informācija, kas tiek savākta no ārējiem avotiem, tajā skaitā informācija, ko sniedz trešās personas, kuras sniedz IKT pakalpojumus, par incidentiem, kas skar to sistēmas un tīklus, un citi informācijas avoti, kurus finanšu vienības uzskata par svarīgiem. Ja šāda informācija ir personas dati, piemēro Savienības tiesību aktus par datu aizsardzību. Personas dati būtu jāierobežo līdz tam, kas ir nepieciešams incidentu atklāšanai.

(20) Lai atvieglotu ar IKT saistītu incidentu atklāšanu, finanšu vienībām būtu jāsaglabā pierādījumi par šiem incidentiem. Lai nodrošinātu, no vienas puses, ka šādi pierādījumi tiek glabāti pietiekami ilgi, un, no otras puses, lai izvairītos no pārmērīga normatīvā sloga, finanšu vienībām būtu jānosaka glabāšanas periods, cita starpā ņemot vērā datu kritiskumu un glabāšanas prasības, kas izriet no Savienības tiesību aktiem.

(21) Lai nodrošinātu, ka ar IKT saistītie incidenti tiek atklāti laikus, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāuzskata, ka noteiktie kritēriji ar IKT saistītu incidentu identificēšanai un reaģēšanai uz tiem nav izsmeļoši. Turklāt, lai gan finanšu vienībām būtu jāņem vērā katrs no šiem kritērijiem, kritērijos aprakstītajiem apstākļiem nebūtu jānotiek vienlaikus, un, lai aktivizētu ar IKT saistītu incidentu atklāšanas un reaģēšanas procesus, būtu pienācīgi jāņem vērā skarto IKT pakalpojumu nozīmīgums.

(22) Izstrādājot IKT darbības nepārtrauktības politiku, šīs regulas II sadaļā minētajām finanšu vienībām būtu jāņem vērā IKT riska pārvaldības būtiskie komponenti, tajā skaitā ar IKT saistīto incidentu pārvaldības un paziņošanas stratēģijas, IKT izmaiņu pārvaldības process un riski, kas saistīti ar trešām personām, kuras sniedz IKT pakalpojumus.

(23) Ir jānosaka scenāriju kopums, kas šīs regulas II sadaļā minētajām finanšu vienībām būtu jāņem vērā, gan īstenojot IKT reaģēšanas un seku novēršanas plānus, gan testējot IKT darbības nepārtrauktības plānus. Minētajiem scenārijiem vajadzētu būt sākumpunktam, no kura finanšu vienības analizē gan katra scenārija atbilstību un ticamību, gan vajadzību izstrādāt alternatīvus scenārijus. Finanšu vienībām būtu jāpievērš īpaša uzmanība tiem scenārijiem, kuros investīcijas noturības pasākumos varētu būt efektīvākas un lietderīgākas. Testējot pārslēgšanos starp primāro IKT infrastruktūru un jebkuru rezerves jaudu, rezerves kopijām un rezerves mehānismiem, finanšu vienībām būtu jānovērtē, vai šī jauda, kopijas un mehānismi darbojas efektīvi pietiekami ilgu laiku, un jānodrošina, ka tiek atjaunota normāla primārās IKT infrastruktūras darbība saskaņā ar atgūšanas mērķiem.

(24) Ir jānosaka prasības attiecībā uz operacionālo risku un jo īpaši prasības IKT projektu un izmaiņu pārvaldībai un IKT darbības nepārtrauktības pārvaldībai, pamatojoties uz prasībām, kas jau ir piemērojamas centrālajiem darījumu partneriem, centrālajiem vērtspapīru depozitārijiem un tirdzniecības vietām saskaņā ar attiecīgi Eiropas Parlamenta un Padomes Regulām (ES) Nr. 648/2012 ([3]), (ES) Nr. 600/2014 ([4]) un (ES) Nr. 909/2014 ([5]).

(25) Saskaņā ar Regulas (ES) 2022/2554 6. panta 5. punktu finanšu vienībām ir jāpārskata sava IKT riska pārvaldības sistēma un jāiesniedz to kompetentajai iestādei ziņojums par šo pārskatīšanu. Lai kompetentās iestādes varētu viegli apstrādāt šajos ziņojumos ietverto informāciju un lai garantētu pienācīgu šīs informācijas nosūtīšanu, finanšu vienībām minētie ziņojumi būtu jāiesniedz elektroniskā formātā, kurā ir iespējams veikt meklēšanu.

(26) Prasībām attiecībā uz finanšu vienībām, uz kurām attiecas Regulas (ES) 2022/2554 16. pantā minētā vienkāršotā IKT riska pārvaldības sistēma, būtu jāvērš uz tām būtiskajām jomām un elementiem, kas, ņemot vērā šo finanšu vienību mērogu, risku, lielumu un sarežģītību, ir minimums, kurš nepieciešams, lai nodrošinātu šo finanšu vienību datu un pakalpojumu konfidencialitāti, integritāti, pieejamību un autentiskumu. Šajā saistībā minētajām finanšu vienībām būtu jāievieš iekšējā pārvaldības un kontroles sistēma ar skaidriem pienākumiem, lai būtu iespējama efektīva un pārdomāta riska pārvaldības sistēma. Turklāt, lai mazinātu administratīvo un darbības slogu, šīm finanšu vienībām būtu jāizstrādā un jādokumentē tikai viena politika, tas ir, informācijas drošības politika, kurā nosaka augsta līmeņa principus un noteikumus, kas nepieciešami, lai aizsargātu šo finanšu vienību datu un pakalpojumu konfidencialitāti, integritāti, pieejamību un autentiskumu.

(27) Šīs regulas noteikumi attiecas uz IKT riska pārvaldības sistēmas jomu, sīki nosakot konkrētos elementus, kas piemērojami finanšu vienībām saskaņā ar Regulas (ES) 2022/2554 15. pantu, un izveidojot vienkāršoto IKT riska pārvaldības sistēmu finanšu vienībām, kas aprakstīta minētās regulas 16. panta 1. punktā. Lai nodrošinātu saskanību starp parasto un vienkāršoto IKT riska pārvaldības sistēmu un ņemot vērā, ka vienlaikus piemērojamiem būtu jākļūst minētajiem noteikumiem, ir lietderīgi iekļaut minētos noteikumus vienā tiesību aktā.

(28) Šī regula ir balstīta uz regulatīvo tehnisko standartu projektu, ko Komisijai iesniegusi Eiropas Banku iestāde, Eiropas Apdrošināšanas un aroda pensiju iestāde un Eiropas Vērtspapīru un tirgu iestāde (turpmāk "Eiropas uzraudzības iestādes"), apspriežoties ar Eiropas Savienības Kiberdrošības aģentūru (*ENISA*).

([3]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 648/2012 (2012. gada 4. jūlijs) par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (OV L 201, 27.7.2012., 1. lpp., ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 600/2014 (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 173, 12.6.2014., 84. lpp., ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 909/2014 (2014. gada 23. jūlijs) par vērtspapīru norēķinu uzlabošanu Eiropas Savienībā, centrālajiem vērtspapīru depozitārijiem un grozījumiem Direktīvās 98/26/EK un 2014/65/ES un Regulā (ES) Nr. 236/2012 (OV L 257, 28.8.2014., 1. lpp., ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Eiropas uzraudzības iestāžu apvienotā komiteja, kas minēta Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 ([6]) 54. pantā, Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1094/2010 ([7]) 54. pantā un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1095/2010 ([8]) 54. pantā, ir rīkojusi atklātu sabiedrisko apspriešanu par regulatīvajiem tehniskajiem standartiem, uz kuriem balstīta šī regula, analizējusi ierosināto standartu potenciālās izmaksas un radītos ieguvumus un lūgusi padomu no Banku nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Regulas (ES) Nr. 1093/2010 37. pantu, Apdrošināšanas un pārapdrošināšanas nozares ieinteresēto personu grupas un Aroda pensiju nozares ieinteresēto personu grupas, kas izveidotas saskaņā ar Regulas (ES) Nr. 1094/2010 37. pantu, un Vērtspapīru un tirgu nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Regulas (ES) Nr. 1095/2010 37. pantu.

(30) Ciktāl, lai izpildītu šajā aktā noteiktos pienākumus, ir vajadzīga personas datu apstrāde, būtu pilnībā jāpiemēro Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([9]) un (ES) 2018/1725 ([10]). Piemēram, ja, lai nodrošinātu incidentu pienācīgu atklāšanu, tiek vākti personas dati, būtu jāievēro datu minimizācijas princips. Par šā akta projekta tekstu ir arī notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju,

IR PIEŅĒMUSI ŠO REGULU.

I SADAĻA

VISPĀRĪGAIS PRINCIPS

1. pants

Vispārējais riska profils un sarežģītība

Izstrādājot un īstenojot IKT drošības politiku, procedūras, protokolus un rīkus, kas minēti II sadaļā, un vienkāršoto IKT riska pārvaldības sistēmu, kas minēta III sadaļā, ņem vērā finanšu vienības lielumu un vispārējo riska profilu un tās pakalpojumu, pasākumu un darbību veidu, mērogu un palielinātas vai samazinātas sarežģītības elementus, tajā skaitā elementus, kas saistīti ar:

a) šifrēšanu un kriptogrāfiju;

b) IKT darbību drošību;

c) tīkla drošību;

([6]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1094/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un aroda pensiju iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/79/EK (OV L 331, 15.12.2010., 48. lpp., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1095/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Vērtspapīru un tirgu iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/77/EK (OV L 331, 15.12.2010., 84. lpp., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) IKT projektu un izmaiņu pārvaldību;

e) IKT riska potenciālo ietekmi uz datu konfidencialitāti, integritāti un pieejamību un traucējumu potenciālo ietekmi uz finanšu vienības darbību nepārtrauktību un pieejamību.

II SADAĻA

IKT RISKA PĀRVALDĪBAS RĪKU, METOŽU, PROCESU UN POLITIKAS TĀLĀKA SASKAŅOŠANA SASKAŅĀ AR REGULAS (ES) 2022/2554 15. PANTU

I NODAĻA

IKT drošības politika, procedūras, protokoli un rīki

1. iedaļa

2. pants

IKT drošības politikas, procedūru, protokolu un rīku vispārējie elementi

1. Finanšu vienības nodrošina, ka to IKT drošības politika, informācijas drošība un saistītās procedūras, protokoli un rīki, kas minēti Regulas (ES) 2022/2554 9. panta 2. punktā, ir integrēti to IKT riska pārvaldības sistēmā. Finanšu vienības ievieš IKT drošības politiku, procedūras, protokolus un rīkus, kas noteikti šajā nodaļā un kas:

a) nodrošina tīklu drošību;

b) ietver aizsardzību pret ielaušanos sistēmā un datu ļaunprātīgu izmantošanu;

c) saglabā datu pieejamību, autentiskumu, integritāti un konfidencialitāti, arī izmantojot kriptogrāfijas metodes;

d) garantē datu precīzu un ātru pārraidi bez būtiskiem traucējumiem un nepamatotiem kavējumiem.

2. Finanšu vienības nodrošina, ka 1. punktā minētā IKT drošības politika:

a) ir pielāgota finanšu vienības informācijas drošības mērķiem, kas noteikti Regulas (ES) 2022/2554 6. panta 8. punktā minētajā digitālās darbības noturības stratēģijā;

b) norāda datumu, kad vadības struktūra formāli apstiprinājusi IKT drošības politiku;

c) ietver rādītājus un pasākumus, lai:

i) uzraudzītu IKT drošības politikas, procedūru, protokolu un rīku īstenošanu;

ii) reģistrētu izņēmumus attiecībā uz šo īstenošanu;

iii) nodrošinātu, ka tiek garantēta finanšu vienības digitālās darbības noturība ii) punktā minēto izņēmumu gadījumā;

d) skaidri nosaka darbinieku atbildību visos līmeņos, lai nodrošinātu finanšu vienības IKT drošību;

e) skaidri nosaka sekas, kādas rodas, ja finanšu vienības darbinieki neievēro IKT drošības politiku, ja noteikumi šajā sakarā nav paredzēti citā finanšu vienības politikā;

f) nosaka uzturamās dokumentācijas sarakstu;

g) skaidri nosaka uzdevumu sadalījumu saistībā ar trīs aizsardzības līniju modeli vai attiecīgi citu iekšējās riska pārvaldības un kontroles modeli, lai izvairītos no interešu konfliktiem;

h) ņem vērā paraugpraksi un attiecīgā gadījumā standartus, kas noteikti Regulas (ES) Nr. 1025/2012 2. panta 1. punktā;

i) nosaka uzdevumus un atbildību par IKT drošības politikas, procedūru, protokolu un rīku izstrādi, īstenošanu un uzturēšanu;

j) tiek pārskatīta saskaņā ar Regulas (ES) 2022/2554 6. panta 5. punktu;

k) ņem vērā būtiskās izmaiņas saistībā ar finanšu vienību, tajā skaitā būtiskās izmaiņas finanšu vienības darbībās vai procesos, kiberdraudu vidē vai piemērojamos juridiskajos pienākumos.

2. iedaļa

3. pants

IKT riska pārvaldība

Finanšu vienības izstrādā, dokumentē un īsteno IKT riska pārvaldības politiku un procedūras, kas ietver visus no šiem elementiem:

a) norāde par riska tolerances līmeņa IKT riskam, kas noteikts saskaņā ar Regulas (ES) 2022/2554 6. panta 8. punkta b) apakšpunktu, apstiprināšanu;

b) procedūra un metodika IKT riska novērtējuma veikšanai, norādot:

   i) ievainojamību un apdraudējumus, kas ietekmē vai var ietekmēt atbalstītās darbības funkcijas, IKT sistēmas un IKT aktīvus, kas atbalsta šīs funkcijas;

   ii) kvantitatīvos vai kvalitatīvos rādītājus i) apakšpunktā minētās ievainojamības un apdraudējumu ietekmes un varbūtības novērtēšanai;

c) procedūra, ko izmanto, lai noteiktu, īstenotu un dokumentētu IKT riska risinājumu pasākumus attiecībā uz identificētajiem un novērtētajiem IKT riskiem, tajā skaitā noteiktu IKT riska risinājumu pasākumus, kas nepieciešami, lai panāktu, ka IKT risks atbilst a) punktā minētajam riska tolerances līmenim;

d) attiecībā uz atlikušajiem IKT riskiem, kas joprojām pastāv pēc c) punktā minēto IKT riska risinājumu pasākumu īstenošanas:

   i) noteikumi par šo atlikušo IKT risku identificēšanu;

   ii) uzdevumu un atbildības noteikšana attiecībā uz:

      1) to atlikušo IKT risku pieņemšanu, kuri pārsniedz a) punktā minēto finanšu vienības riska tolerances līmeni;

      2) pārskatīšanas procesu, kas minēts šā d) punkta iv) apakšpunktā;

   iii) pieņemto atlikušo IKT risku inventarizācijas izstrāde, ietverot pamatojumu to pieņemšanai;

   iv) noteikumi par pieņemto atlikušo IKT risku pārskatīšanu vismaz reizi gadā, ietverot:

      1) norādi par jebkādām atlikušo IKT risku izmaiņām;

      2) pieejamo risku mazināšanas pasākumu novērtējumu;

      3) novērtējumu par to, vai iemesli, kas pamato atlikušo IKT risku pieņemšanu, joprojām ir spēkā un piemērojami pārskatīšanas datumā;

e) noteikumi par to, kā uzrauga:

   i) jebkādas izmaiņas IKT risku un kiberdraudu vidē;

   ii) iekšējo un ārējo ievainojamību un apdraudējumus;

   iii) finanšu vienības IKT risku, lai varētu ātri atklāt izmaiņas, kas varētu ietekmēt tās IKT riska profilu;

f) noteikumi par procesu, ar kuru nodrošina, ka tiek ņemtas vērā jebkādas izmaiņas finanšu vienības darbības stratēģijā un digitālās darbības noturības stratēģijā.

Pirmās daļas c) punkta nolūkos minētajā punktā norādītā procedūra nodrošina:

a) īstenoto IKT riska risinājuma pasākumu efektivitātes uzraudzību;

b) novērtējumu par to, vai ir sasniegti finanšu vienības noteiktie riska tolerances līmeņi;

c) novērtējumu par to, vai finanšu vienība ir veikusi darbības, lai vajadzības gadījumā koriģētu vai uzlabotu minētos pasākumus.

3. iedaļa

IKT aktīvu pārvaldība

4. pants

IKT aktīvu pārvaldības politika

1. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno IKT aktīvu pārvaldības politiku.

2. Šā panta 1. punktā minētā IKT aktīvu pārvaldības politika:

a) paredz saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu identificēto un klasificēto IKT aktīvu aprites cikla uzraudzību un pārvaldību;

b) paredz, ka finanšu vienības veic uzskaiti par visu turpmāk minēto:

i) katra IKT aktīva unikālais identifikators;

ii) informācija par visu IKT aktīvu fizisko vai loģisko atrašanās vietu;

iii) visu IKT aktīvu klasifikācija, kā minēts Regulas (ES) 2022/2254 8. panta 1. punktā;

iv) IKT aktīvu īpašnieku identitāte;

v) IKT aktīva atbalstītās uzņēmējdarbības funkcijas vai pakalpojumi;

vi) IKT darbības nepārtrauktības prasības, tajā skaitā atgūšanas laika mērķi un atgūšanas punkta mērķi;

vii) vai IKT aktīvs var būt vai ir pakļauts ārējiem tīkliem, tajā skaitā internetam;

viii) saiknes un savstarpējā atkarība starp IKT aktīviem un uzņēmējdarbības funkcijām, kas izmanto katru IKT aktīvu;

ix) attiecīgā gadījumā par visiem IKT aktīviem – trešo personu, kas sniedz pakalpojumus, parasto, paplašināto un pielāgoto atbalsta pakalpojumu beigu datumi, pēc kuriem šos IKT aktīvus to piegādātājs vai trešā persona, kas sniedz IKT pakalpojumus, vairs neatbalsta;

c) attiecībā uz finanšu vienībām, kas nav mikrouzņēmumi, paredz, ka šīm finanšu vienībām jāveic tās informācijas uzskaite, kas nepieciešama, lai veiktu īpašu IKT riska novērtējumu par visām mantotajām IKT sistēmām, kas minētas Regulas (ES) 2022/2554 8. panta 7. punktā.

5. pants

IKT aktīvu pārvaldības procedūra

1. Finanšu vienības izstrādā, dokumentē un īsteno IKT aktīvu pārvaldības procedūru.

2. Šā panta 1. punktā minētajā IKT aktīvu pārvaldības procedūrā nosaka kritērijus, pēc kuriem veic informācijas aktīvu un IKT aktīvu, kas atbalsta uzņēmējdarbības funkcijas, kritiskuma novērtējumu. Minētajā novērtējumā ņem vērā:

a) IKT risku, kas saistīts ar minētajām uzņēmējdarbības funkcijām un to atkarību no informācijas aktīviem vai IKT aktīviem;

b) to, kā šādu informācijas aktīvu un IKT aktīvu konfidencialitātes, integritātes un pieejamības zaudēšana ietekmētu finanšu vienības uzņēmējdarbības procesus un darbības.

4. iedaļa

Šifrēšana un kriptogrāfija

6. pants

Šifrēšanas un kriptogrāfijas kontroles

1. Kā daļu no savas Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno šifrēšanas un kriptogrāfijas kontroles politiku.

2. Finanšu vienības izstrādā 1. punktā minēto šifrēšanas un kriptogrāfijas kontroļu politiku, pamatojoties uz apstiprinātas datu klasifikācijas un IKT riska novērtējuma rezultātiem. Minētā politika ietver noteikumus par visu turpmāk minēto:

a) glabāšanā vai pārsūtīšanā esošu datu šifrēšana;

b) ja nepieciešams, lietošanā esošu datu šifrēšana;

c) iekšējo tīklu savienojumu un datplūsmas ar ārējām personām šifrēšana;

d) 7. pantā minētā šifrēšanas atslēgu pārvaldība, paredzot noteikumus par kriptogrāfijas atslēgu pareizu izmantošanu, aizsardzību un aprites ciklu.

Šā panta b) punkta nolūkos, ja lietošanā esošu datu šifrēšana nav iespējama, finanšu vienības apstrādā lietošanā esošus datus nodalītā un aizsargātā vidē vai veic līdzvērtīgus pasākumus, lai nodrošinātu datu konfidencialitāti, integritāti, autentiskumu un pieejamību.

3. Finanšu vienības iekļauj 1. punktā minētajā šifrēšanas un kriptogrāfijas kontroļu politikā kritērijus kriptogrāfijas metožu un izmantošanas prakses atlasei, ņemot vērā paraugpraksi un standartus, kas noteikti Regulas (ES) Nr. 1025/2012 2. panta 1. punktā, un attiecīgo IKT aktīvu klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu. Finanšu vienības, kas nespēj ievērot paraugpraksi vai standartus vai izmantot uzticamākās metodes, pieņem riska mazināšanas un uzraudzības pasākumus, kas nodrošina noturību pret kiberdraudiem.

4. Finanšu vienības iekļauj 1. punktā minētajā šifrēšanas un kriptogrāfijas kontroļu politikā noteikumus par kriptogrāfijas tehnoloģijas atjaunināšanu vai, ja nepieciešams, mainīšanu, pamatojoties uz norisēm kriptoanalīzes jomā. Minētie atjauninājumi vai maiņa nodrošina, ka kriptogrāfijas tehnoloģija joprojām ir noturīga pret kiberdraudiem, kā prasīts 10. panta 2. punkta a) apakšpunktā. Finanšu vienības, kas nespēj atjaunināt vai mainīt kriptogrāfijas tehnoloģiju, pieņem riska mazināšanas un uzraudzības pasākumus, kas nodrošina noturību pret kiberdraudiem.

5. Finanšu vienības iekļauj 1. punktā minētajā šifrēšanas un kriptogrāfijas kontroļu politikā prasību reģistrēt riska mazināšanas un uzraudzības pasākumus, kas pieņemti saskaņā ar 3. un 4. punktu, un sniegt pamatotu skaidrojumu par to, kāpēc tas darīts.

7. pants

Kriptogrāfijas atslēgu pārvaldība

1. Finanšu vienības iekļauj 6. panta 2. punkta d) apakšpunktā minētajā kriptogrāfijas atslēgu pārvaldības politikā prasības par kriptogrāfijas atslēgu pārvaldību visā to aprites ciklā, ieskaitot šo kriptogrāfijas atslēgu ģenerēšanu, atjaunošanu, glabāšanu, dublēšanu, arhivēšanu, izgūšanu, pārsūtīšanu, norakstīšanu, anulēšanu un iznīcināšanu.

2. Finanšu vienības nosaka un īsteno kontroles, lai aizsargātu kriptogrāfijas atslēgas visā to aprites ciklā pret neatļautu piekļuvi, izpaušanu un pārveidošanu. Finanšu vienības izstrādā minētās kontroles, pamatojoties uz apstiprinātas datu klasifikācijas un IKT riska novērtējuma rezultātiem.

3. Finanšu vienības izstrādā un īsteno metodes kriptogrāfijas atslēgu aizstāšanai to nozaudēšanas gadījumā vai ja ar atslēgām ir veiktas neatļautas manipulācijas, vai tās ir bojātas.

4. Finanšu vienības izveido un uztur reģistru, kurā reģistrē visus sertifikātus un sertifikātu glabāšanas ierīces, vismaz attiecībā uz IKT aktīviem, kas atbalsta kritiski svarīgas vai svarīgas funkcijas. Finanšu vienības pastāvīgi atjaunina minēto reģistru.

5. Finanšu vienības nodrošina sertifikātu ātru atjaunošanu pirms to derīguma termiņa beigām.

5. iedaļa

IKT darbību drošība

8. pants

Politika un procedūras attiecībā uz IKT darbībām

1. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno IKT darbību pārvaldības politiku un procedūras. Minētajā politikā un procedūrās skaidri nosaka, kā finanšu vienības ekspluatē, uzrauga, kontrolē un atjauno savus IKT aktīvus, ietverot IKT darbību dokumentēšanu.

2. Šā panta 1. punktā minētajā IKT darbību politikā un procedūrā iekļauj visus šos elementus:

a) IKT aktīvu apraksts, ietverot visu turpmāk minēto:

   i) prasības attiecībā uz IKT sistēmas drošu instalēšanu, uzturēšanu, konfigurēšanu un atinstalēšanu;

   ii) prasības attiecībā uz IKT aktīvu izmantoto informācijas aktīvu pārvaldību, tajā skaitā to apstrādi un darbībām ar tiem – gan automatizētām, gan manuālām;

   iii) prasības attiecībā uz mantoto IKT sistēmu identifikāciju un kontroli;

b) IKT sistēmu kontroles un uzraudzība, ietverot visu turpmāk minēto:

   i) prasības attiecībā uz IKT sistēmu rezerves kopiju veidošanu un atjaunošanu;

   ii) grafiku veidošanas prasības, ņemot vērā IKT sistēmu savstarpējo atkarību;

   iii) protokoli revīzijas izsekojamības un sistēmu žurnāla informācijai;

   iv) prasības, lai nodrošinātu, ka iekšējās revīzijas un citas testēšanas veikšana līdz minimumam samazina traucējumus uzņēmējdarbībā;

   v) prasības par IKT ražošanas vides nodalīšanu no izstrādes, testēšanas un citām neražošanas vidēm;

   vi) prasības veikt izstrādi un testēšanu vidēs, kas ir nodalītas no ražošanas vides;

   vii) prasības veikt izstrādi un testēšanu ražošanas vidēs;

c) kļūdu apstrāde saistībā ar IKT sistēmām, ietverot visu turpmāk minēto:

i) procedūras un protokoli kļūdu apstrādei;

ii) kontaktpersonas, kuras sniedz atbalstu un kurām ziņot, tajā skaitā ārējā atbalsta kontaktpersonas, pie kurām vērsties neparedzētu darbības vai tehnisku jautājumu gadījumā;

iii) IKT sistēmu restartēšanas, atrites un atgūšanas procedūras izmantošanai IKT sistēmu traucējumu gadījumā.

Šā punkta b) apakšpunkta v) punkta nolūkos nodalīšanā ņem vērā visus vides komponentus, tajā skaitā kontus, datus vai savienojumus, kā prasīts 13. panta pirmās daļas a) punktā.

Šā punkta b) apakšpunkta vii) punkta nolūkos 1. punktā minētā politika un procedūras nodrošina, ka gadījumi, kad testēšanu veic ražošanas vidē, ir skaidri identificēti, pamatoti, ir uz ierobežotu laiku un ka tos apstiprinājusi attiecīgā funkcija saskaņā ar 16. panta 6. punktu. Finanšu vienības nodrošina IKT sistēmu un ražošanas datu pieejamību, konfidencialitāti, integritāti un autentiskumu izstrādes un testēšanas darbību laikā ražošanas vidē.

9. pants

Jaudas un veiktspējas pārvaldība

1. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno jaudas un veiktspējas pārvaldības procedūras attiecībā uz turpmāk norādīto:

a) to IKT sistēmu jaudas prasību identifikācija;

b) resursu optimizācijas piemērošana;

c) uzraudzības procedūras, lai uzturētu un uzlabotu:

i) datu un IKT sistēmu pieejamību;

ii) IKT sistēmu efektivitāti;

iii) IKT jaudas trūkuma novēršanu.

2. Šā panta 1. punktā minētās jaudas un veiktspējas pārvaldības procedūras nodrošina, ka finanšu vienības veic pasākumus, kas ir atbilstoši, lai ņemtu vērā to IKT sistēmu specifiku, kam ir ilgi vai sarežģīti iepirkuma vai apstiprināšanas procesi vai kas ir resursietilpīgas.

10. pants

Ievainojamības un ielāpu pārvaldība

1. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno ievainojamības pārvaldības procedūras.

2. Šā panta 1. punktā minētās ievainojamības pārvaldības procedūras:

a) nosaka un atjaunina nozīmīgus un uzticamus informācijas resursus, lai veidotu un uzturētu informētību par ievainojamību;

b) nodrošina automatizētas ievainojamības skenēšanas un IKT aktīvu novērtējumu veikšanu, kur šo darbību biežums un tvērums ir samērīgs ar klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un ar IKT aktīva vispārējo riska profilu;

c) pārbauda, vai:

i) trešās personas, kas sniedz IKT pakalpojumus, rīkojas attiecībā uz ievainojamību, kas saistīta ar finanšu vienībai sniegtajiem IKT pakalpojumiem;

ii) minētie pakalpojumu sniedzēji laikus ziņo finanšu vienībai vismaz par kritisku ievainojamību un statistiku un tendencēm;

d) seko līdzi tam, kā izmanto:

i) trešo personu bibliotēkas, tajā skaitā atklātā pirmkoda bibliotēkas, ko izmanto IKT pakalpojumi, kuri atbalsta kritiskas vai svarīgas funkcijas;

ii) IKT pakalpojumus, ko izstrādājusi pati finanšu vienība vai ko finanšu vienībai īpaši pielāgojusi vai izstrādājusi trešā persona, kura sniedz IKT pakalpojumus;

e) nosaka procedūras atbildīgai ievainojamības atklāšanai klientiem, darījumu partneriem un sabiedrībai;

f) nosaka ielāpu un citu riska mazināšanas pasākumu izvēršanas prioritātes identificētās ievainojamības risināšanai;

g) uzrauga un verificē ievainojamības izlabošanu;

h) pieprasa, lai tiek reģistrēta jebkura atklātā ievainojamība, kas ietekmē IKT sistēmas, un tiek uzraudzīta ievainojamības atrisināšana.

Šā punkta b) apakšpunkta nolūkos finanšu vienības vismaz reizi nedēļā veic automatizētu ievainojamības skenēšanu un novērtējumus par IKT aktīviem, kas atbalsta kritiski svarīgas vai svarīgas funkcijas.

Šā punkta c) apakšpunkta nolūkos finanšu vienības pieprasa, lai trešās personas, kas sniedz IKT pakalpojumus, izmeklē attiecīgo ievainojamību, noskaidro cēloņus un īsteno attiecīgus riska mazināšanas pasākumus.

Šā punkta d) apakšpunkta nolūkos finanšu vienības, attiecīgā gadījumā sadarbojoties ar trešo personu, kas sniedz IKT pakalpojumus, uzrauga trešo personu bibliotēku versiju un iespējamos atjauninājumus. Attiecībā uz gataviem (plašpatēriņa) IKT aktīviem vai IKT aktīvu komponentiem, kas iegādāti un ko izmanto tādu IKT pakalpojumu darbībā, kuri neatbalsta kritiski svarīgas vai svarīgas funkcijas, finanšu vienības, ciktāl iespējams, seko līdzi trešo personu bibliotēku, tajā skaitā atklātā pirmkoda bibliotēku, izmantojumam.

Šā punkta f) apakšpunkta nolūkos finanšu vienības ņem vērā ievainojamības kritiskumu, klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un identificētās ievainojamības ietekmēto IKT aktīvu riska profilu.

3. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno ielāpu pārvaldības procedūras.

4. Šā panta 3. punktā minētās ielāpu pārvaldības procedūras:

a) ciktāl iespējams, izmantojot automatizētus rīkus, identificē un izvērtē pieejamos programmatūras un aparatūras ielāpus un atjauninājumus;

b) nosaka ārkārtas rīcības procedūras attiecībā uz IKT aktīvu ielāpiem un atjauninājumiem;

c) testē un ievieš programmatūras un aparatūras ielāpus un atjauninājumus, kas minēti 8. panta 2. punkta b) apakšpunkta v), vi) un vii) punktā;

d) nosaka termiņus programmatūras un aparatūras ielāpu un atjauninājumu instalēšanai un eskalācijas procedūras gadījumam, ja šos termiņus nevar ievērot.

11. pants

Datu un sistēmu drošība

1. Kā daļu no Regulas (ES) 2022/2554 9. panta 2. punktā minētās IKT drošības politikas, procedūrām, protokoliem un rīkiem finanšu vienības izstrādā, dokumentē un īsteno datu un sistēmu drošības procedūru.

2. Šā panta 1. punktā minētā datu un sistēmu drošības procedūra ietver visus turpmāk uzskaitītos elementus, kas saistīti ar datu un IKT sistēmu drošību, atbilstoši klasifikācijai, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu:

a) šīs regulas 21. pantā minētie piekļuves ierobežojumi, kas atbalsta aizsardzības prasības katram klasifikācijas līmenim;

b) drošas bāzkonfigurācijas identifikācija IKT aktīviem, kas mazina šo IKT aktīvu pakļaušanu kiberdraudiem, un pasākumi, lai regulāri pārbaudītu, vai šī bāzkonfigurācija tiek efektīvi izmantota;

c) drošības pasākumu identifikācija, lai nodrošinātu, ka IKT sistēmās un galapunkta ierīcēs tiek instalēta tikai atļauta programmatūra;

d) drošības pasākumu identifikācija aizsardzībai pret ļaunprātīgiem kodiem;

e) drošības pasākumu identifikācija, lai nodrošinātu, ka finanšu vienības datu pārsūtīšanai un glabāšanai tiek izmantoti tikai atļauti datu nesēji, sistēmas un galapunkta ierīces;

f) šādas prasības, lai aizsargātu pārnēsājamu galapunkta ierīču un privātu nepārnēsājamu galapunkta ierīču izmantošanu:

   i) prasība izmantot pārvaldības risinājumu, lai attālināti pārvaldītu galapunkta ierīces un attālināti dzēstu finanšu vienības datus;

   ii) prasība izmantot drošības mehānismus, ko neatļautā veidā nevar pārveidot, atcelt vai apiet darbinieki vai trešās personas, kuras sniedz IKT pakalpojumus;

   iii) prasība izmantot noņemamus datu nesējus tikai tad, ja atlikušais IKT risks joprojām ir finanšu vienības riska tolerances līmenī, kas minēts 3. panta pirmās daļas a) punktā;

g) process to datu drošai dzēšanai, kas tiek turēti finanšu vienības telpās vai tiek glabāti ārēji un ko finanšu vienībai vairs nav nepieciešams vākt vai glabāt;

h) process to datu glabāšanas ierīču drošai utilizācijai vai izņemšanai no ekspluatācijas, kas atrodas finanšu vienības telpās vai tiek glabātas ārēji un kas satur konfidenciālu informāciju;

i) drošības pasākumu identifikācija un īstenošana, lai novērstu datu zaudēšanu vai noplūdi attiecībā uz sistēmām un galapunkta ierīcēm;

j) drošības pasākumu īstenošana, lai nodrošinātu, ka tāldarbs un privātu galapunkta ierīču izmantošana nelabvēlīgi neietekmē finanšu vienības IKT drošību;

k) attiecībā uz IKT aktīviem vai pakalpojumiem, ko pārvalda trešā persona, kura sniedz IKT pakalpojumus, – prasību identifikācija un īstenošana, lai uzturētu digitālās darbības noturību, saskaņā ar datu klasifikācijas un IKT riska novērtējuma rezultātiem.

Šā punkta b) apakšpunkta nolūkos minētajā apakšpunktā norādītajā drošajā konfigurācijā ņem vērā paraugpraksi un atbilstošas metodes, kas noteiktas standartos, kuri definēti Regulas (ES) Nr. 1025/2012 2. panta 1. punktā.

Šā punkta k) apakšpunkta nolūkos finanšu vienības ņem vērā:

a) piegādātāju ieteikto iestatījumu īstenošanu attiecībā uz elementiem, ko pārvalda finanšu vienība;

b) ar informācijas drošību saistīto uzdevumu un atbildības skaidru sadali starp finanšu vienību un trešo personu, kas sniedz IKT pakalpojumus, saskaņā ar principu, kas nosaka, ka finanšu vienībai ir pilna atbildība par trešo personu, kas tai sniedz IKT pakalpojumus un kas minēta Regulas (ES) 2022/2554 28. panta 1. punkta a) apakšpuktā, un par finanšu vienībām, kas minētas norādītās regulas 28. panta 2. punktā, un saskaņā ar finanšu vienības politiku attiecībā uz to IKT pakalpojumu izmantošanu, kas atbalsta kritiskas vai svarīgas funkcijas;

c) vajadzību nodrošināt un uzturēt finanšu vienībā atbilstošas kompetences izmantotā pakalpojuma pārvaldībā un drošībā;

d) tehniskos un organizatoriskos pasākumus, lai mazinātu riskus, kas saistīti ar infrastruktūru, kuru trešā persona, kas sniedz IKT pakalpojumus, izmanto saviem IKT pakalpojumiem, ņemot vērā paraugpraksi un standartus, kas noteikti Regulas (ES) Nr. 1025/2012 2. panta 1. punktā.

12. pants

Reģistrēšana

1. Finanšu vienības kā daļu no pasākumiem aizsardzībai pret ielaušanos sistēmā un datu ļaunprātīgu izmantošanu izstrādā, dokumentē un īsteno reģistrēšanas procedūras, protokolus un rīkus.

2. Šā panta 1. punktā minētajās reģistrēšanas procedūrās, protokolos un rīkos iekļauj visus šos elementus:

a) ierakstāmo notikumu identifikācija, žurnālu glabāšanas periods un pasākumi žurnāla datu aizsardzībai un apstrādei, ņemot vērā mērķi, kādam ieraksti tiek izveidoti;

b) žurnālu detalizācijas pakāpes pielāgošana to mērķim un izmantojumam, lai varētu efektīvi atklāt anomālas darbības, kā minēts 24. pantā;

c) prasība reģistrēt notikumus, kas saistīti ar visu turpmāk minēto:

   i) loģiskās un fiziskās piekļuves kontrole, kā minēts 21. pantā, un identitātes pārvaldība;

   ii) jaudas pārvaldība;

   iii) izmaiņu pārvaldība;

   iv) IKT darbības, tajā skaitā IKT sistēmu darbības;

   v) tīklu datplūsmas darbības, tajā skaitā IKT tīklu veiktspēja;

d) pasākumi, lai aizsargātu reģistrēšanas sistēmas un žurnālu informāciju pret manipulācijām, dzēšanu un neatļautu piekļuvi, kad dati tiek glabāti, pārsūtīti vai attiecīgā gadījumā tiek lietoti;

e) pasākumi reģistrēšanas sistēmu atteiču atklāšanai;

f) neskarot nekādas piemērojamās normatīvās prasības saskaņā ar Savienības vai valsts tiesību aktiem – finanšu vienības katras IKT sistēmas pulksteņu sinhronizācija, pamatojoties uz dokumentētu, uzticamu atsauces laika avotu.

Šā punkta a) apakšpunkta nolūkos finanšu vienības nosaka glabāšanas periodu, ņemot vērā darbības un informācijas drošības mērķus, iemeslu, kādēļ notikums tiek reģistrēts žurnālos, un IKT riska novērtējuma rezultātus.

6. iedaļa

Tīkla drošība

13. pants

Tīkla drošības pārvaldība

Finanšu vienības kā daļu no aizsardzības pasākumiem, kas nodrošina tīklu aizsardzību pret ielaušanos sistēmā un datu ļaunprātīgu izmantošanu, izstrādā, dokumentē un īsteno politiku, procedūras, protokolus un rīkus attiecībā uz tīkla drošības pārvaldību, kas ietver visu turpmāk minēto:

a) IKT sistēmu un tīklu nošķiršana un segmentācija, ņemot vērā:

   i) šo IKT sistēmu un tīklu atbalstītās funkcijas kritiskumu vai svarīgumu;

   ii) klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu;

   iii) IKT aktīvu, kas izmanto šīs IKT sistēmas un tīklus, vispārējo riska profilu;

b) visu finanšu vienības tīkla savienojumu un datu plūsmu dokumentācija;

c) atsevišķa un specializēta tīkla izmantošana IKT aktīvu pārvaldībai;

d) tīkla piekļuves kontroļu identifikācija un īstenošana, lai novērstu un atklātu jebkuras neatļautas ierīces vai sistēmas vai jebkura finanšu vienības drošības prasībām neatbilstoša gala punkta savienojumu ar finanšu vienības tīklu;

e) to tīkla savienojumu šifrēšana, kuri notiek pa uzņēmuma tīkliem, publiskajiem tīkliem, mājas tīkliem, trešo personu tīkliem un bezvadu tīkliem, attiecībā uz izmantotajiem komunikācijas protokoliem, ņemot vērā apstiprinātās datu klasifikācijas rezultātus, IKT riska novērtējuma rezultātus un 6. panta 2. punktā minēto tīkla savienojumu šifrēšanu;

f) tīklu izstrāde saskaņā ar finanšu vienības noteiktajām IKT drošības prasībām, ņemot vērā paraugpraksi, lai nodrošinātu tīkla konfidencialitāti, integritāti un pieejamību;

g) tīkla datplūsmas aizsardzība starp iekšējiem tīkliem un internetu un citiem ārējiem savienojumiem;

h) uzdevumu un atbildības, un veicamo pasākumu identifikācija, lai konkrēti noteiktu, īstenotu, apstiprinātu, mainītu un pārskatītu ugunsmūra noteikumus un savienojumu filtrus;

i) tīkla arhitektūras un tīkla drošības sistēmas pārskatīšana reizi gadā un – mikrouzņēmumiem – periodiski, lai apzinātu iespējamo ievainojamību;

j) pasākumi, lai vajadzības gadījumā īslaicīgi izolētu apakštīklus un tīkla komponentus un ierīces;

k) visu tīkla komponentu drošas bāzkonfigurācijas īstenošana un tīkla un tīkla ierīču stiprināšana atbilstīgi jebkuriem piegādātāju norādījumiem, attiecīgā gadījumā – piemērojamiem standartiem, kas noteikti Regulas (ES) Nr. 1025/2012 2. panta 1. punktā, un paraugpraksi;

l) procedūras, lai ierobežotu, nobloķētu un izbeigtu sistēmas sesijas un attālās sesijas pēc noteikta neaktivitātes perioda;

m) attiecībā uz tīkla pakalpojumu līgumiem:

   i) IKT un informācijas drošības pasākumu, pakalpojumu līmeņu un visu tīkla pakalpojumu pārvaldības prasību identifikācija un specifikācija;

   ii) vai šos pakalpojumus sniedz IKT pakalpojumu sniedzējs grupas iekšienē vai trešās personas, kas sniedz IKT pakalpojumus.

Šā punkta h) apakšpunkta nolūkos finanšu vienības veic ugunsmūra noteikumu un savienojumu filtru regulāru pārskatīšanu saskaņā ar klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un iesaistīto IKT sistēmu vispārējo riska profilu. Attiecībā uz IKT sistēmām, kas atbalsta kritiski svarīgas vai svarīgas funkcijas, finanšu vienības pārbauda esošo ugunsmūra noteikumu un savienojumu filtru atbilstību vismaz reizi sešos mēnešos.

14. pants

Pārsūtītās informācijas aizsardzība

1. Kā daļu no aizsardzības pasākumiem, ko veic, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, finanšu vienības izstrādā, dokumentē un īsteno politiku, procedūras, protokolus un rīkus pārsūtītās informācijas aizsardzībai. Finanšu vienības jo īpaši nodrošina visu turpmāk minēto:

a) datu pieejamība, autentiskums, integritāte un konfidencialitāte pārsūtīšanā pa tīkliem un procedūru noteikšana, lai novērtētu atbilstību šīm prasībām;

b) datu noplūžu novēršana un atklāšana un informācijas droša pārsūtīšana starp finanšu vienību un ārējām personām;

c) prasības attiecībā uz konfidencialitātes vai neizpaušanas pasākumiem, kas atspoguļo finanšu vienības vajadzības pēc informācijas aizsardzības gan finanšu vienības darbiniekiem, gan trešo personu darbiniekiem, tie īstenotas, dokumentētas un regulāri pārskatītas.

2. Finanšu vienības izstrādā 1. punktā minēto politiku, procedūras, protokolus un rīkus pārsūtītās informācijas aizsardzībai, pamatojoties uz apstiprinātas datu klasifikācijas un IKT riska novērtējuma rezultātiem.

7. iedaļa

IKT projektu un izmaiņu pārvaldība

15. pants

IKT projektu pārvaldība

1. Kā daļu no aizsardzības pasākumiem, ko veic, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, finanšu vienības izstrādā, dokumentē un īsteno IKT projektu pārvaldības politiku.

2. Šā panta 1. punktā minētā IKT projektu pārvaldības politika nosaka elementus, kas nodrošina to IKT projektu efektīvu pārvaldību, kuri saistīti ar finanšu vienības IKT sistēmu iegādi, uzturēšanu un attiecīgā gadījumā izstrādi.

3. Šā panta 1. punktā minētā IKT projektu pārvaldības politika ietver visu turpmāk minēto:

a) IKT projekta mērķi;

b) IKT projekta pārvaldība, tajā skaitā uzdevumi un atbildība;

c) IKT projekta plānošana, grafiks un posmi;

d) IKT projekta riska novērtējums;

e) attiecīgie atskaites punkti;

f) izmaiņu pārvaldības prasības;

g) visu prasību (ieskaitot drošības prasības) testēšana un attiecīgais apstiprinājuma process, kad IKT sistēma tiek ieviesta ražošanas vidē.

4. Šā panta 1. punktā minētā IKT projektu pārvaldības politika nodrošina IKT projektu drošu īstenošanu, sniedzot nepieciešamo informāciju un zinātību no uzņēmējdarbības jomas vai funkcijām, ko ietekmē IKT projekts.

5. Saskaņā ar 3. punkta d) apakšpunktā minēto IKT projektu riska novērtējumu 1. punktā minētā IKT projektu pārvaldības politika nodrošina, ka par to IKT projektu izveidi un norisi, kuri ietekmē finanšu vienības kritiski svarīgas vai svarīgas funkcijas, un par to saistītajiem riskiem tiek paziņots vadības struktūrai šādi:

a) atsevišķi vai par visiem kopā atkarībā no IKT projektu svarīguma un lieluma;

b) periodiski un, ja nepieciešams, balstoties uz katru notikumu.

16. pants

IKT sistēmu iegāde, izstrāde un uzturēšana

1. Kā daļu no aizsardzības pasākumiem, ko veic, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, finanšu vienības izstrādā, dokumentē un īsteno politiku, kas reglamentē IKT sistēmu iegādi, izstrādi un uzturēšanu. Minētā politika:

a) nosaka drošības praksi un metodiku saistībā ar IKT sistēmu iegādi, izstrādi un uzturēšanu;

b) prasa, lai tiktu identificētas:

   i) tehniskās specifikācijas un IKT tehniskās specifikācijas, kas definētas Regulas (ES) Nr. 1025/2012 2. panta 4. un 5. punktā;

   ii) prasības saistībā ar IKT sistēmu iegādi, izstrādi un uzturēšanu, īpašu uzmanību pievēršot IKT drošības prasībām un to apstiprināšanai, ko veic attiecīgā darbības funkcija un IKT aktīvu īpašnieks saskaņā ar finanšu vienības iekšējo pārvaldības kārtību;

c) nosaka pasākumus, lai mazinātu IKT sistēmu nejaušas pārveides vai tīšu manipulāciju ar tām risku, kad šīs IKT sistēmas tiek izstrādātas, uzturētas un ieviestas ražošanas vidē.

2. Finanšu vienības izstrādā, dokumentē un īsteno IKT sistēmu iegādes, izstrādes un uzturēšanas procedūru visu IKT sistēmu testēšanai un apstiprināšanai pirms to izmantošanas un pēc uzturēšanas saskaņā ar 8. panta 2. punkta b) apakšpunkta v), vi) un vii) punktu. Testēšanas līmenis ir samērīgs ar darbības procedūru un attiecīgo IKT aktīvu kritiskumu. Testēšanu plāno tā, lai pārbaudītu, vai jaunas IKT sistēmas ir atbilstošas, lai darbotos, kā paredzēts, tajā skaitā pārbaudītu iekšēji izstrādātas programmatūras kvalitāti.

Centrālie darījumu partneri papildus pirmajā daļā noteiktajām prasībām pirmajā daļā minētajā testēšanas plānošanā un veikšanā pēc vajadzības iesaista:

a) tīrvērtes dalībniekus un klientus;

b) sadarbspējīgus centrālos darījumu partnerus;

c) citas ieinteresētās personas.

Centrālie vērtspapīru depozitāriji papildus pirmajā daļā noteiktajām prasībām pirmajā daļā minētajā testēšanas plānošanā un veikšanā pēc vajadzības iesaista:

a) lietotājus;

b) kritiski svarīgus sabiedrisko pakalpojumu sniedzējus un kritiski svarīgus pakalpojumu sniedzējus;

c) citus centrālos vērtspapīru depozitārijus;

d) citas tirgus infrastruktūras;

e) jebkuras citas iestādes, ar kurām centrālajiem vērtspapīru depozitārijiem ir identificēta savstarpējā atkarība to uzņēmējdarbības nepārtrauktības politikā.

3. Šā panta 2. punktā minētā procedūra ietver pirmkodu pārskatīšanu, kas aptver gan statisko, gan dinamisko testēšanu. Minētā testēšana ietver internetā izmantotu sistēmu un lietojumprogrammu drošības testēšanu saskaņā ar 8. panta 2. punkta b) apakšpunkta v), vi) un vii) punktu. Finanšu vienības:

a) identificē un analizē pirmkoda ievainojamību un anomālijas;

b) pieņem rīcības plānu šīs ievainojamības un anomāliju risināšanai;

c) uzrauga minētā rīcības plāna īstenošanu.

4. Šā panta 2. punktā minētā procedūra ietver programmatūras pakotņu drošības testēšanu, ko veic ne vēlāk kā integrācijas posmā saskaņā ar 8. panta 2. punkta b) apakšpunkta v), vi) un vii) punktu.

5. Šā panta 2. punktā minētā procedūra nodrošina, ka:

a) neražošanas vide glabā tikai anonimizētus, pseidonimizētus vai randomizētus ražošanas datus;

b) finanšu vienībām ir jāaizsargā datu integritāte un konfidencialitāte neražošanas vidēs.

6. Atkāpjoties no 5. punkta, 2. punktā minētā procedūra var noteikt, ka ražošanas dati tiek glabāti tikai īpašiem testēšanas gadījumiem, ierobežotu laikposmu un pēc attiecīgās funkcijas apstiprinājuma un šādu gadījumu paziņošanas IKT riska pārvaldības funkcijai.

7. Šā panta 2. punktā minētā procedūra ietver kontroļu īstenošanu, lai aizsargātu to IKT sistēmu pirmkoda integritāti, kuras tiek izstrādātas iekšēji vai kuras izstrādā trešā persona, kas sniedz IKT pakalpojumus, un kuras finanšu vienībai nodod trešā persona, kas sniedz IKT pakalpojumus.

8. Šā panta 2. punktā minētā procedūra paredz, ka īpašniekprogrammatūra un, ja iespējams, pirmkods, ko nodrošinājušas trešās personas, kuras sniedz IKT pakalpojumus, vai kas tiek saņemti no pirmkoda projektiem, pirms to ieviešanas ražošanas vidē ir jāanalizē un jātestē saskaņā ar 3. punktu.

9. Šā panta 1.–8. punktu attiecina arī uz IKT sistēmām, ko izstrādājuši vai pārvalda lietotāji ārpus IKT funkcijas, izmantojot uz risku balstītu pieeju.

17. pants

IKT izmaiņu pārvaldība

1. Kā daļu no aizsardzības pasākumiem, ko veic, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, finanšu vienības IKT izmaiņu pārvaldības procedūrās, kas minētas Regulas (ES) 2022/2554 9. panta 4. punkta e) apakšpunktā, attiecībā uz visām programmatūras, aparatūras, aparātprogrammatūras komponentu, sistēmu vai drošības parametru izmaiņām iekļauj visus šos elementus:

a) pārbaude par to, vai ir izpildītas IKT drošības prasības;

b) mehānismi, lai nodrošinātu to funkciju neatkarību, kuras apstiprina izmaiņas, un to funkciju neatkarību, kuras atbild par minēto izmaiņu pieprasīšanu un īstenošanu;

c) uzdevumu un atbildības skaidrs apraksts, lai nodrošinātu, ka:

   i) izmaiņas tiek konkrēti noteiktas un plānotas;

   ii) ir plānota atbilstoša pāreja;

   iii) izmaiņas tiek testētas un pabeigtas kontrolētā vidē;

   iv) pastāv efektīva kvalitātes nodrošināšana;

d) izmaiņu datu dokumentēšana un paziņošana, tajā skaitā:

   i) izmaiņu mērķis un tvērums;

   ii) termiņš izmaiņu īstenošanai;

   iii) paredzamie rezultāti;

e) darbības nepārtrauktības procedūru un atbildības identifikācija, tajā skaitā procedūras un atbildība par izmaiņu atcelšanu vai atgūšanos pēc izmaiņām, kas īstenotas neveiksmīgi;

f) procedūras, protokoli un rīki ārkārtas izmaiņu pārvaldībai, kas nodrošina pienācīgu aizsardzību;

g) procedūras, lai dokumentētu, atkārtoti izvērtētu, novērtētu un apstiprinātu ārkārtas izmaiņas pēc to īstenošanas, ieskaitot aprisinājumus un ielāpus;

h) izmaiņu potenciālās ietekmes uz esošajiem IKT drošības pasākumiem identifikācija un novērtējums par to, vai šādu izmaiņu dēļ ir jāpieņem papildu IKT drošības pasākumi.

2. Pēc būtisku izmaiņu ieviešanas savās IKT sistēmas centrālie darījumu partneri un centrālie vērtspapīru depozitāriji pakļauj savas IKT sistēmas stingrai testēšanai, kurā simulē stresa apstākļus.

Centrālie darījumu partneri pirmajā daļā minētajā testēšanas plānošanā un veikšanā pēc vajadzības iesaista:

a) tīrvērtes dalībniekus un klientus;

b) sadarbspējīgus centrālos darījumu partnerus;

c) citas ieinteresētās personas.

Centrālie vērtspapīru depozitāriji pirmajā daļā minētajā testēšanas plānošanā un veikšanā pēc vajadzības iesaista:

a) lietotājus;

b) kritiski svarīgus sabiedrisko pakalpojumu sniedzējus un kritiski svarīgus pakalpojumu sniedzējus;

c) citus centrālos vērtspapīru depozitārijus;

d) citas tirgus infrastruktūras;

e) jebkuras citas iestādes, ar kurām centrālajiem vērtspapīru depozitārijiem ir identificēta savstarpējā atkarība to IKT darbības nepārtrauktības politikā.

8. iedaļa

18. pants

Fiziskā un vides drošība

1. Kā daļu no aizsardzības pasākumiem, ko veic, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, finanšu vienības precīzi nosaka, dokumentē un īsteno fiziskās un vides drošības politiku. Finanšu vienības izstrādā minēto politiku, ņemot vērā kiberdraudu vidi, saskaņā ar klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un ņemot vērā IKT aktīvu un piekļūstamu informācijas aktīvu vispārējo riska profilu.

2. Šā panta 1. punktā minētā fiziskās un vides drošības politika ietver visu turpmāk minēto:

a) atsauce uz politikas iedaļu par piekļuves pārvaldības tiesību kontroli, kas minēta 21. panta pirmās daļas g) punktā;

b) pasākumi, lai pret uzbrukumiem, negadījumiem un vides draudiem un apdraudējumiem aizsargātu finanšu vienības telpas, datu centrus un vietas, ko finanšu vienība noteikusi par sensitīvām un kur atrodas IKT aktīvi un informācijas aktīvi;

c) pasākumi, lai aizsargātu IKT aktīvus gan finanšu vienības telpās, gan ārpus tām, ņemot vērā IKT riska novērtējuma rezultātus saistībā ar attiecīgajiem IKT aktīviem;

d) pasākumi, lai nodrošinātu finanšu vienības IKT aktīvu, informācijas aktīvu un fiziskās piekļuves kontroles ierīču pieejamību, autentiskumu, integritāti un konfidencialitāti, veicot atbilstošu uzturēšanu;

e) pasākumi, lai saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, tajā skaitā:

   i) "tīra galda" politika attiecībā uz dokumentiem;

   ii) "tīra ekrāna" politika attiecībā uz informācijas apstrādes ierīcēm.

Šā punkta b) apakšpunkta nolūkos pasākumi aizsardzībai pret vides draudiem un apdraudējumiem ir samērīgi ar telpu, datu centru, par sensitīvām noteikto vietu svarīgumu un tajās notiekošo darbību vai esošo IKT sistēmu kritiskumu.

Šā punkta c) apakšpunkta nolūkos 1. punktā minētā fiziskās un vides drošības politika ietver pasākumus, lai pienācīgi aizsargātu bez uzraudzības esošus IKT aktīvus.

II NODAĻA

Cilvēkresursu politika un piekļuves kontrole

19. pants

Cilvēkresursu politika

Finanšu vienības savā cilvēkresursu politikā vai citā attiecīgā politikā ietver visus šādus ar IKT drošību saistītus elementus:

a) jebkādas īpašas atbildības par IKT drošību identifikācija un uzticēšana;

b) prasības finanšu vienības un trešo personu, kas sniedz IKT pakalpojumus, darbiniekiem, kuri izmanto finanšu vienības IKT aktīvus vai tiem piekļūst:

i) iepazīties ar finanšu vienības IKT drošības politiku, procedūrām un protokoliem un tos ievērot;

ii) zināt par ziņošanas kanāliem, ko finanšu vienība izveidojusi, lai atklātu anomālu uzvedību, tajā skaitā attiecīgā gadījumā par ziņošanas kanāliem, kas izveidoti atbilstīgi Eiropas Parlamenta un Padomes Direktīvai (ES) 2019/1937 ([11]);

iii) izbeidzot darba attiecības, nodot finanšu vienībai visus to rīcībā esošos IKT aktīvus un materiālos informācijas aktīvus, kas pieder finanšu vienībai.

20. pants

Identitātes pārvaldība

1. Lai varētu piešķirt lietotāja piekļuves tiesības saskaņā ar 21. pantu, kā daļu no savas piekļuves pārvaldības tiesību kontroles finanšu vienības izstrādā, dokumentē un īsteno identitātes pārvaldības politiku un procedūras, kas nodrošina to fizisko personu un sistēmu unikālu identificēšanu un autentificēšanu, kuras piekļūst finanšu vienību informācijai.

2. Šā panta 1. punktā minētajā identitātes pārvaldības politikā un procedūrās iekļauj visus šos elementus:

a) neskarot 21. panta pirmās daļas c) punktu, katram finanšu vienības darbiniekam vai trešo personu, kas sniedz IKT pakalpojumus, darbiniekam, kurš piekļūst finanšu vienības informācijas aktīviem un IKT aktīviem, piešķir unikālu identitāti, kas atbilst unikālam lietotāja kontam;

b) identitāšu un kontu aprites cikla pārvaldības process, kas pārvalda visu kontu izveidi, izmaiņas tajos, to pārskatīšanu un atjaunināšanu, pagaidu dezaktivizāciju un slēgšanu.

Šā punkta a) apakšpunkta nolūkos finanšu vienības veic visu piešķirto identitāšu uzskaiti. Minēto uzskaiti glabā pēc finanšu vienības reorganizācijas vai pēc līgumattiecību izbeigšanas, neskarot piemērojamos Savienības un valsts tiesību aktos noteiktās glabāšanas prasības.

Šā punkta b) apakšpunkta nolūkos, ja tas ir iespējams un atbilstoši, finanšu vienības ievieš automatizētus risinājumus aprites cikla identitātes pārvaldības procesam.

21. pants

Piekļuves kontrole

Kā daļu no savas piekļuves pārvaldības tiesību kontroles finanšu vienības izstrādā, dokumentē un īsteno politiku, kas ietver visus no šiem elementiem:

a) IKT piekļuves tiesību piešķiršana, pamatojoties uz principiem "vajadzība zināt", "vajadzība izmantot" un mazāko tiesību principu, arī attiecībā uz attālu piekļuvi un piekļuvi ārkārtas gadījumā;

b) uzdevumu nošķiršana, lai novērstu nepamatotu piekļuvi kritiski svarīgiem datiem vai novērstu tādu piekļuves tiesību kombināciju piešķiršanu, ko var izmantot kontroļu apiešanai;

c) noteikums par lietotāja pārskatatbildību, ciktāl iespējams, ierobežojot vispārējo un dalīto lietotāja kontu izmantošanu un nodrošinot, ka lietotāji vienmēr ir identificējami attiecībā uz darbībām, kas veiktas IKT sistēmās;

([11]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1937 (2019. gada 23. oktobris) par to personu aizsardzību, kuras ziņo par Savienības tiesību aktu pārkāpumiem (OV L 305, 26.11.2019., 17. lpp., ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) noteikums par ierobežojumiem piekļuvei IKT aktīviem, izklāstot kontroles un rīkus neatļautas piekļuves novēršanai;

e) kontu pārvaldības procedūras, lai piešķirtu, mainītu vai atsauktu piekļuves tiesības lietotāju un vispārējiem kontiem, tajā skaitā vispārējiem administratoru kontiem, ietverot noteikumu par visu turpmāk minēto:

i) uzdevumu un atbildības piešķiršana par piekļuves tiesību piešķiršanu, pārskatīšanu un atsaukšanu;

ii) privileģētas, ārkārtas un administratora piekļuves piešķiršana, pamatojoties uz vajadzību zināt vai uz *ad hoc* pamata, attiecībā uz visām IKT sistēmām;

iii) piekļuves tiesību tūlītēja atsaukšana darba attiecību izbeigšanas gadījumā vai ja piekļuve vairs nav nepieciešama;

iv) piekļuves tiesību atjaunināšana, kad ir nepieciešamas izmaiņas un vismaz gadā attiecībā uz visām IKT sistēmām, izņemot IKT sistēmas, kas atbalsta kritiskas vai svarīgas funkcijas, un vismaz reizi sešos mēnešos attiecībā uz IKT sistēmām, kas atbalsta kritiskas vai svarīgas funkcijas;

f) autentifikācijas metodes, ietverot visus šos elementus:

i) autentifikācijas metožu izmantošana, kas ir samērīga ar klasifikāciju, kura noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un ar IKT aktīvu vispārējo riska profilu, arī ņemot vērā paraugpraksi;

ii) spēcīgu autentifikācijas metožu izmantošana saskaņā ar paraugpraksi un metodēm attiecībā uz attālu piekļuvi finanšu vienības tīklam, privileģētu piekļuvi, piekļuvi IKT aktīviem, kas atbalsta kritiskas vai svarīgas funkcijas, vai IKT aktīviem, kas ir publiski pieejami;

g) fiziskās piekļuves kontroles pasākumi, tajā skaitā:

i) to fizisko personu identifikācija un reģistrēšana žurnālā, kurām ir atļauts piekļūt telpām, datu centriem un finanšu vienības par sensitīvām noteiktām vietām, kur atrodas IKT un informācijas aktīvi;

ii) fiziskās piekļuves kritiskiem IKT aktīviem piešķiršana tikai pilnvarotām personām saskaņā ar principu "vajadzība zināt" un mazāko tiesību principu un uz *ad hoc* pamata;

iii) uzraudzība attiecībā uz fizisko piekļuvi telpām, datu centriem un finanšu vienības par sensitīvām noteiktām vietām, kur atrodas IKT un informācijas aktīvi, vai abi;

iv) fiziskās piekļuves tiesību pārskatīšana, lai nodrošinātu, ka nevajadzīgas piekļuves tiesības tiek steidzīgi atsauktas.

Šā punkta e) apakšpunkta i) punkta nolūkos finanšu vienības nosaka glabāšanas periodu, ņemot vērā darbības un informācijas drošības mērķus, iemeslus, kādēļ notikums tiek reģistrēts žurnālos, un IKT riska novērtējuma rezultātus.

Šā punkta e) apakšpunkta ii) punkta nolūkos finanšu vienības, ja iespējams, izmanto speciālus kontus administratīvu uzdevumu veikšanai IKT sistēmās. Ja tas ir iespējams un atbilstoši, finanšu vienības ievieš automatizētus risinājumus privileģētas piekļuves pārvaldībai.

Šā punkta g) apakšpunkta i) punkta nolūkos identifikācija un reģistrēšana žurnālos ir samērīga ar telpu, datu centru, par sensitīvām noteikto vietu svarīgumu un tajās notiekošo darbību vai esošo IKT sistēmu kritiskumu.

Šā punkta g) apakšpunkta iii) punkta nolūkos uzraudzība ir samērīga ar klasifikāciju, kas noteikta saskaņā ar Regulas (ES) 2022/2554 8. panta 1. punktu, un vietas, kurai piekļūst, kritiskumu.

III NODAĻA

Ar IKT saistītu incidentu atklāšana un reaģēšana uz tiem

22. pants

Ar IKT saistītu incidentu pārvaldības politika

Kā daļu no mehānismiem, kurus izmanto anomālu darbību atklāšanai, ieskaitot IKT tīklu veiktspējas problēmas un ar IKT saistītus incidentus, finanšu vienības izstrādā, dokumentē un īsteno ar IKT saistītu incidentu politiku, ar kuras starpniecību tās:

a) dokumentē ar IKT saistītu incidentu pārvaldības procesu, kas minēts Regulas (ES) 2022/2554 17. pantā;

b) izveido sarakstu, kurā iekļautas attiecīgās kontaktpersonas ar iekšējām funkcijām un ārējās ieinteresētās personas, kas tieši iesaistītas IKT darbības drošībā, arī attiecībā uz:

   i) kiberdraudu atklāšanu un uzraudzību;

   ii) anomālu darbību atklāšanu;

   iii) ievainojamības pārvaldību;

c) nosaka, īsteno un izmanto tehniskos, organizatoriskos un darbības mehānismus, lai atbalstītu ar IKT saistītu incidentu pārvaldības procesu, tajā skaitā mehānismus, kas ļauj ātri atklāt anomālas darbības un uzvedību saskaņā ar šīs regulas 23. pantu;

d) glabā visus pierādījumus par incidentiem, kas saistīti ar IKT, ne ilgāk kā nepieciešams nolūkiem, kuriem dati savākti, samērīgi ar ietekmēto darbības funkciju, atbalsta procesu un IKT un informācijas aktīvu kritiskumu un saskaņā ar Komisijas Deleģētās regulas (ES) 2024/1772 ([12]) 15. pantu un ar jebkuru piemērojamo datu glabāšanas prasību atbilstīgi Savienības tiesību aktiem;

e) nosaka un īsteno mehānismus, lai analizētu būtiskus vai atkārtotus ar IKT saistītus incidentus un tendences ar IKT saistītu incidentu skaita un atkārtošanās ziņā.

Šā panta d) punkta nolūkos finanšu vienības minētajā punktā norādītos pierādījumus glabā drošā veidā.

23. pants

Anomālu darbību atklāšana un kritēriji ar IKT saistītu incidentu atklāšanai un reaģēšanai uz tiem

1. Finanšu vienības nosaka skaidrus uzdevumus un atbildību, lai varētu efektīvi atklāt ar IKT saistītus incidentus un anomālas darbības un reaģēt uz tiem.

2. Mehānisms, ko izmanto, lai ātri atklātu anomālas darbības, tajā skaitā IKT tīklu veiktspējas problēmas un ar IKT saistītus incidentus, un kas minēts Regulas (ES) 2022/2554 10. panta 1. punktā, ļauj finanšu vienībām:

a) apkopot, uzraudzīt un analizēt:

   i) iekšējus un ārējus faktorus, tajā skaitā vismaz žurnālu ierakstus, kas savākti saskaņā ar šīs regulas 12. pantu, informāciju no darbības un IKT funkcijām, un visas problēmas, par kurām ziņo finanšu vienības lietotāji;

   ii) iespējamos iekšējos un ārējos kiberdraudus, ņemot vērā scenārijus, ko visbiežāk izmanto draudu īstenotāji, un scenārijus, kas balstīti uz draudu izlūkošanas darbību;

([12]) Komisijas Deleģētā regula (ES) 2024/1772 (2024. gada 13. marts), ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem, kuros precizēti kritēriji ar IKT saistītu incidentu un kiberdraudu klasifikācijai, nosakot būtiskuma robežvērtības un precizējot sīkāku informāciju, kas ietverama ziņojumos par būtiskiem incidentiem (OV L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) ar IKT saistītu incidentu paziņojumus, ko sniedz trešā persona, kura finanšu vienībai sniedz IKT pakalpojumus, par incidentiem, kas atklāti IKT sistēmās un tīklos un kas var ietekmēt finanšu vienību;

b) identificēt anomālas darbības un uzvedību un ieviest rīkus, kas ģenerē brīdinājumus par anomālām darbībām un uzvedību, vismaz attiecībā uz tiem IKT aktīviem un informācijas aktīviem, kas atbalsta kritiski svarīgas vai svarīgas funkcijas;

c) noteikt b) apakšpunktā minēto brīdinājumu prioritātes, lai varētu pārvaldīt atklātos ar IKT saistītos incidentus paredzamajā problēmas atrisināšanas laikā, ko noteikušas finanšu vienības, gan darba laikā, gan ārpus darba laika;

d) automātiski vai manuāli reģistrēt, analizēt un izvērtēt visu būtisko informāciju par visām anomālajām darbībām un uzvedību.

Šā punkta b) apakšpunkta nolūkos minētajā punktā norādītie rīki ietver rīkus, kas sniedz automatizētus brīdinājumus, balstoties uz iepriekš definētiem noteikumiem, lai identificētu anomālijas, kas ietekmē datu avotu vai žurnālu apkopojuma pilnīgumu un integritāti.

3. Finanšu vienības aizsargā visus anomālu darbību ierakstus pret manipulācijām un neatļautas piekļuves tiem, kad tie tiek glabāti, tiek nosūtīti vai attiecīgā gadījumā tiek izmantoti.

4. Finanšu vienības reģistrē visu būtisko informāciju par katru atklāto anomālo darbību tā, lai būtu iespējams:

a) identificēt anomālās darbības veikšanas datumu un laiku;

b) identificēt anomālās darbības atklāšanas datumu un laiku;

c) identificēt anomālās darbības veidu.

5. Lai aktivizētu ar IKT saistītu incidentu atklāšanas un reaģēšanas procesus, kas minēti Regulas (ES) 2022/2554 10. panta 2. punktā, finanšu vienības ņem vērā visus šos kritērijus:

a) norādes, ka ļaunprātīgā darbība var būt veikta IKT sistēmā vai tīklā vai ka šāda IKT sistēma vai tīkls var būt apdraudēti;

b) datu zudumi, kas atklāti saistībā ar datu pieejamību, autentiskumu, integritāti un konfidencialitāti;

c) atklātā nelabvēlīgā ietekme uz finanšu vienības darījumiem un darbībām;

d) IKT sistēmu un tīklu nepieejamība.

6. Šā punkta 5. punkta nolūkos finanšu vienības arī ņem vērā ietekmēto pakalpojumu kritiskumu.

IV NODAĻA

IKT darbības nepārtrauktības pārvaldība

24. pants

IKT darbības nepārtrauktības politikas elementi

1. Finanšu vienības savā IKT darbības nepārtrauktības politikā, kas minēta Regulas (ES) 2022/2554 11. panta 1. punktā, ietver visus no šiem elementiem:

a) apraksts par:

i) IKT darbības nepārtrauktības politikas mērķiem, tajā skaitā savstarpējo saistību starp IKT darbības nepārtrauktību un vispārējo darbības nepārtrauktību, arī ņemot vērā Regulas (ES) 2022/2554 11. panta 5. punktā minētās uzņēmējdarbības ietekmes analīzes (UIA) rezultātus;

ii) IKT darbības nepārtrauktības kārtības, plānu, procedūru un mehānismu tvērumu, ietverot ierobežojumus un izņēmumus;

iii) laikposmu, kas jāaptver ar IKT darbības nepārtrauktības kārtību, plāniem, procedūrām un mehānismiem;

iv) kritērijiem IKT darbības nepārtrauktības plānu, IKT reaģēšanas un seku novēršanas plānu un krīzes paziņošanas plānu aktivizēšanai un dezaktivizēšanai;

b) noteikumi par:

i) pārvaldību un organizāciju IKT darbības nepārtrauktības politikas īstenošanai, tajā skaitā uzdevumiem, atbildību un eskalācijas procedūrām, kas nodrošina, ka ir pieejami pietiekami resursi;

ii) IKT darbības nepārtrauktības plānu un vispārējo darbības nepārtrauktības plānu saskaņošanu, ietverot vismaz visus no šiem elementiem:

1) iespējamie atteiču scenāriji, tajā skaitā scenāriji, kas minēti šīs regulas 26. panta 2. punktā;

2) atgūšanas mērķi, norādot, ka finanšu vienība spēj atjaunot tās kritisko vai svarīgo funkciju darbības pēc traucējumiem atbilstīgi atgūšanas laika mērķim un atgūšanas punkta mērķim;

iii) IKT darbības nepārtrauktības plānu izstrādi nopietniem uzņēmējdarbības traucējumiem kā daļu no šiem plāniem un IKT darbības nepārtrauktības pasākumu prioritāšu noteikšanu, izmantojot uz risku balstītu pieeju;

iv) IKT reaģēšanas un seku novēršanas plānu izstrādi, testēšanu un pārskatīšanu saskaņā ar šīs regulas 25. un 26. pantu;

v) īstenotās IKT darbības nepārtrauktības kārtības, plānu, procedūru un mehānismu efektivitātes pārskatīšanu saskaņā ar šīs regulas 26. pantu;

vi) IKT darbības nepārtrauktības politikas saskaņošanu ar:

1) saziņas politiku, kas minēta Regulas (ES) 2022/2554 14. panta 2. punktā;

2) saziņas un krīzes pārvarēšanas pasākumiem, kas minēti Regulas (ES) 2022/2554 11. panta 2. punkta e) apakšpunktā.

2. Papildus 1. punktā minētajām prasībām centrālie darījumu partneri nodrošina, ka to IKT darbības nepārtrauktības politika:

a) paredz to kritiski svarīgo funkciju atgūšanas maksimālo laiku, kas nepārsniedz divas stundas;

b) ņem vērā ārējās saites un savstarpējo atkarību finanšu infrastruktūrās, tajā skaitā centrālā darījumu partnera apstiprinātās tirdzniecības vietas, vērtspapīru norēķinu un maksājumu sistēmas un kredītiestādes, ko izmanto centrālais darījumu partneris vai saistīts centrālais darījumu partneris;

c) paredz, ka ir jābūt ieviestai kārtībai, lai:

i) nodrošinātu centrālā darījumu partnera kritisko vai svarīgo funkciju nepārtrauktību, pamatojoties uz negadījumu scenārijiem;

ii) uzturētu rezerves apstrādes vietu, kas spēj nodrošināt centrālā darījumu partnera kritisko vai svarīgo funkciju nepārtrauktību identiski galvenajai vietai;

iii) uzturētu rezerves uzņēmējdarbības vietu vai nodrošinātu tūlītēju piekļuvi tai, lai personāls varētu nodrošināt pakalpojuma nepārtrauktību, ja primārā uzņēmējdarbības vieta nav pieejama;

iv) ņemtu vērā vajadzību pēc papildu datu apstrādes vietām, jo īpaši tad, ja galvenās un rezerves vietas riska profilu dažādība nenodrošina pietiekamu pārliecību, ka centrālā darījumu partnera darbības nepārtrauktības mērķi tiks sasniegti jebkura scenārija gadījumā.

Šā punkta a) apakšpunkta nolūkos centrālie darījumu partneri visos apstākļos izpilda dienas noslēguma procedūras un maksājumus vajadzīgajā laikā un dienā.

Šā punkta c) apakšpunkta i) nolūkos minētajā punktā norādītajā kārtībā ņem vērā pietiekamu cilvēkresursu pieejamību, kritiski svarīgo funkciju maksimālo dīkstāves laiku un kļūmjpārlēci un darbības pārjaunošanu uz rezerves vietu.

Šā punkta c) apakšpunkta ii) punkta nolūkos minētajā punktā norādītajai rezerves apstrādes vietai ir ģeogrāfiskais riska profils, kas atšķiras no galvenās vietas profila.

3. Papildus 1. punktā minētajām prasībām centrālie vērtspapīru depozitāriji nodrošina, ka to IKT darbības nepārtrauktības politika:

a) ņem vērā visas saiknes ar lietotājiem, kritiski svarīgiem sabiedrisko pakalpojumu sniedzējiem un kritiski svarīgiem pakalpojumu sniedzējiem, citiem centrālajiem vērtspapīru depozitārijiem un citām tirgus infrastruktūrām un savstarpējo atkarību no tiem;

b) paredz, ka IKT darbības nepārtrauktības kārtībai ir jānodrošina, ka atgūšanas laika mērķis to kritiski svarīgajām vai svarīgajām funkcijām nav ilgāks par divām stundām.

4. Papildus 1. punktā minētajām prasībām tirdzniecības vietas nodrošina, ka to IKT darbības nepārtrauktības politika nodrošina, ka:

a) tirdzniecību var atjaunot divu stundu vai īsākā laikā pēc traucējumu incidenta;

b) maksimālais datu apjoms, kas var tikt zaudēts no jebkura tirdzniecības vietas IT pakalpojuma pēc traucējumu incidenta, ir tuvu nullei.

25. pants

IKT darbības nepārtrauktības plānu testēšana

1. Testējot IKT darbības nepārtrauktības plānus saskaņā ar Regulas (ES) 2022/2554 11. panta 6. punktu, finanšu vienības ņem vērā finanšu vienības uzņēmējdarbības ietekmes analīzi (UIA) un IKT riska novērtējumu, kas minēts šīs regulas 3. panta 1. punkta b) apakšpunktā.

2. Finanšu vienības, testējot savus IKT darbības nepārtrauktības plānus, kas minēti 1. punktā, novērtē, vai plāni spēj nodrošināt finanšu vienības kritiski svarīgo vai svarīgo funkciju nepārtrauktību. Testēšana:

a) tiek veikta, pamatojoties uz testa scenārijiem, kuros simulē potenciālus traucējumus, ietverot smagu, bet ticamu scenāriju pienācīgu kopumu;

b) attiecīgā gadījumā ietver trešo personu sniegto IKT pakalpojumu testēšanu;

c) attiecībā uz finanšu vienībām, kas nav mikrouzņēmumi, kā minēts Regulas (ES) 2022/2554 11. panta 6. punkta otrajā daļā, ietver scenārijus, kuros notiek pārslēgšanās no galvenās IKT infrastruktūras uz rezerves jaudu, rezerves kopijām un rezerves mehānismiem;

d) tiek plānota tā, lai atspēkotu pieņēmumus, uz kuriem balstīti uzņēmējdarbības nepārtrauktības plāni, tajā skaitā pārvaldības kārtība un krīzes saziņas plāni;

e) ietver procedūras, lai pārbaudītu finanšu vienību darbinieku, trešo personu, kas sniedz IKT pakalpojumus, IKT sistēmu un IKT pakalpojumu spēju pienācīgi reaģēt uz scenārijiem, kas pienācīgi ņemti vērā saskaņā ar 26. panta 2. punktu.

Šā punkta a) apakšpunkta nolūkos finanšu vienības testēšanā vienmēr iekļauj scenārijus, kas apsvērti uzņēmējdarbības nepārtrauktības plānu izstrādei.

Šā punkta b) apakšpunkta nolūkos finanšu vienības attiecīgā gadījumā pienācīgi ņem vērā scenārijus, kas saistīti ar trešo personu, kuras sniedz IKT pakalpojumus, maksātnespēju vai neveiksmēm vai ar politiskiem riskiem trešo personu, kas sniedz IKT pakalpojumus, jurisdikcijās.

Šā punkta c) apakšpunkta nolūkos testēšanā pārbauda, vai vismaz kritiski svarīgās vai svarīgās funkcijas var darboties pietiekamu laiku un vai var atjaunot normālu darbību.

3. Papildus 2. punktā minētajām prasībām centrālie darījumu partneri savu 1. punktā minēto IKT darbības nepārtrauktības plānu testēšanā iesaista:

a) tīrvērtes dalībniekus;

b) ārējus pakalpojumu sniedzējus;

c) attiecīgās iestādes finanšu infrastruktūrā, ar kurām centrālajiem darījumu partneriem ir identificēta savstarpēja atkarība to uzņēmējdarbības nepārtrauktības politikā.

4. Papildus 2. punktā minētajām prasībām centrālie vērtspapīru depozitāriji savu 1. punktā minēto IKT darbības nepārtrauktības plānu testēšanā attiecīgā gadījumā iesaista:

a) centrālo vērtspapīru depozitāriju lietotājus;

b) kritiski svarīgus sabiedrisko pakalpojumu sniedzējus un kritiski svarīgus pakalpojumu sniedzējus;

c) citus centrālos vērtspapīru depozitārijus;

d) citas tirgus infrastruktūras;

e) jebkuras citas iestādes, ar kurām centrālajiem vērtspapīru depozitārijiem ir identificēta savstarpējā atkarība to uzņēmējdarbības nepārtrauktības politikā.

5. Finanšu vienības dokumentē 1. punktā minētās testēšanas rezultātus. Visas no minētās testēšanas izrietošās nepilnības analizē, risina un paziņo vadības struktūrai.

26. pants

IKT reaģēšanas un seku novēršanas plāni

1. Izstrādājot IKT reaģēšanas un seku novēršanas plānus, kas minēti Regulas (ES) 2022/2554 11. panta 3. punktā, finanšu vienības ņem vērā finanšu vienības uzņēmējdarbības ietekmes analīzes (UIA) rezultātus. Minētie IKT reaģēšanas un seku novēršanas plāni:

a) paredz nosacījumus to aktivizēšanai vai dezaktivizēšanai un visus izņēmumus attiecībā uz šādu aktivizēšanu vai dezaktivizēšanu;

b) apraksta, kādas darbības ir veicamas, lai nodrošinātu vismaz to IKT sistēmu un pakalpojumu pieejamību, integritāti, nepārtrauktību un atgūšanu, kas atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas;

c) tiek izstrādāti tā, lai sasniegtu finanšu vienības darbību atjaunošanas plānus;

d) tiek dokumentēti un darīti pieejami darbiniekiem, kuri iesaistīti IKT reaģēšanas un seku novēršanas plānu izpildē, un ir ātri pieejami ārkārtas gadījumā;

e) paredz gan īstermiņa, gan ilgtermiņa atgūšanas iespējas, tajā skaitā sistēmu daļēju atgūšanu;

f) nosaka IKT reaģēšanas un seku novēršanas plānu mērķus un nosacījumus šo plānu atzīšanai par veiksmīgi izpildītiem.

Šā punkta d) apakšpunkta nolūkos finanšu vienības skaidri nosaka uzdevumus un atbildību.

2. Šā panta 1. punktā minētajos IKT reaģēšanas un seku novēršanas plānos identificē attiecīgos scenārijus, tajā skaitā nopietnu uzņēmējdarbības traucējumu un palielinātas traucējumu varbūtības scenārijus. Minētajos plānos scenārijus izstrādā, pamatojoties uz aktuālo informāciju par draudiem un uz gūtajām atziņām no iepriekšējiem darbības pārtraukumiem. Finanšu vienības pienācīgi ņem vērā visus šos scenārijus:

a) kiberuzbrukumi un pārslēgšanās starp primāro IKT infrastruktūru un rezerves jaudu, rezerves kopijām un rezerves mehānismiem;

b) scenāriji, kuros kritiski svarīgas vai svarīgas funkcijas nodrošināšanas kvalitāte pasliktinās līdz nepieņemamam līmenim vai neizdodas, tajos arī pienācīgi ņemot vērā jebkuras attiecīgās trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas vai citu atteiču iespējamo ietekmi;

c) telpu, tajā skaitā biroja un uzņēmējdarbības telpu, un datu centru daļēja vai pilnīga darbības atteice;

d) IKT aktīvu vai komunikācijas infrastruktūras būtiska atteice;

e) kritiska darbinieku skaita vai par darbību nepārtrauktības garantēšanu atbildīgo darbinieku nepieejamība;

f) klimata pārmaiņu un ar vides degradāciju saistītu notikumu, dabas katastrofu, pandēmiju un fizisku uzbrukumu, tajā skaitā ielaušanās sistēmās un teroristu uzbrukumu, ietekme;

g) uzbrukumi no iekšienes;

h) politiskā un sociālā nestabilitāte, attiecīgā gadījumā arī trešās personas, kas sniedz IKT pakalpojumus, jurisdikcijā un vietā, kur notiek datu glabāšana un apstrāde;

i) plaši elektroenerģijas atvienojumi.

3. Ja primārie seku novēršanas pasākumi īstermiņā var nebūt īstenojami izmaksu, risku, loģistikas vai neparedzētu apstākļu dēļ, 1. punktā minētajos IKT reaģēšanas un seku novēršanas plānos apsver alternatīvas iespējas.

4. Kā daļu no 1. punktā minētajiem IKT reaģēšanas un seku novēršanas plāniem finanšu vienības apsver un īsteno pasākumus, lai mazinātu to trešo personu darbības atteices, kuras sniedz IKT pakalpojumus, kas atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas.

V NODAĻA

Ziņojums par IKT riska pārvaldības sistēmas pārskatīšanu

27. pants

Ziņojuma par IKT riska pārvaldības sistēmas pārskatīšanu formāts un saturs

1. Finanšu vienības iesniedz Regulas (ES) 2022/2554 6. panta 5. punktā minēto ziņojumu par IKT riska pārvaldības sistēmas pārskatīšanu elektroniskā formātā, kurā ir iespējams veikt meklēšanu.

2. Finanšu vienības 1. punktā minētajā ziņojumā iekļauj visu šo informāciju:

a) ievada iedaļa, kurā:

i) skaidri norāda finanšu vienību, uz kuru attiecas ziņojums, un attiecīgā gadījumā apraksta tās grupas struktūru;

ii) apraksta ziņojuma kontekstu – finanšu vienības pakalpojumu, pasākumu un darbību veidu, mērogu un sarežģītību, tās organizāciju, identificētas kritiskās funkcijas, stratēģiju, būtiskus notiekošus projektus vai darbības, attiecības un tās atkarību no vietējiem vai nolīgtiem IKT pakalpojumiem un sistēmām vai ietekmi, kāda šādu sistēmu pilnīgai zaudēšanai vai būtiskam darbības pasliktinājumam būtu uz kritiskajām vai svarīgajām funkcijām un tirgus efektivitāti;

iii) sniedz kopsavilkumu par nozīmīgām IKT riska pārvaldības sistēmas izmaiņām kopš iepriekšējā iesniegtā ziņojuma;

iv) ietver izpildvaras līmeņa kopsavilkumu par pašreizējo un īstermiņa IKT profilu, draudu vidi, novērtēto tās kontroļu efektivitāti un finanšu vienības drošības stāvokli;

b) datums, kurā finanšu vienības vadības struktūra apstiprinājusi ziņojumu;

c) apraksts par iemeslu IKT riska pārvaldības sistēmas pārskatīšanai saskaņā ar Regulas (ES) 2022/2554 6. panta 5. punktu;

d) pārskata perioda sākuma un beigu datums;

e) norāde uz funkciju, kas atbild par pārskatīšanu;

f) apraksts par nozīmīgām IKT riska pārvaldības sistēmas izmaiņām un uzlabojumiem kopš iepriekšējās pārskatīšanas;

g) pārskatīšanas konstatējumu kopsavilkums un sīka analīze un novērtējums par vājo vietu, trūkumu un nepilnību smagumu IKT riska pārvaldības sistēmā pārskata periodā;

h) apraksts par pasākumiem, kas veikti, lai novērstu apzinātās vājās vietas, trūkumus un nepilnības, tajā skaitā:

i) kopsavilkums par pasākumiem, kas veikti, lai izlabotu apzinātās vājās vietas, trūkumus un nepilnības;

ii) paredzamais pasākumu īstenošanas datums un datumi saistībā ar īstenošanas iekšējo kontroli, tajā skaitā informācija par minēto pasākumu īstenošanas norisi ziņojuma sagatavošanas dienā, attiecīgā gadījumā paskaidrojot, vai pastāv risks, ka termiņi var netikt ievēroti;

iii) izmantojamie rīki un par pasākumu īstenošanu atbildīgās funkcijas identifikācija, sīki aprakstot, vai šie rīki un funkcijas ir iekšēji vai ārēji;

iv) apraksts par pasākumos paredzēto izmaiņu ietekmi uz finanšu vienības budžeta resursiem, cilvēkresursiem un materiālu resursiem, ieskaitot resursus, kas atvēlēti jebkādu korektīvu pasākumu īstenošanai;

v) informācija par kompetentās iestādes informēšanu (attiecīgā gadījumā);

vi) ja attiecībā uz apzinātajām vājajām vietām, trūkumiem vai nepilnībām nav veikti korektīvi pasākumi – sīks to kritēriju skaidrojums, kas izmantoti, lai analizētu minēto vājo vietu, trūkumu vai nepilnību ietekmi nolūkā izvērtēt atlikušo IKT risku, un sīks to kritēriju skaidrojums, kas izmantoti, lai akceptētu saistīto atlikušo risku;

i) informācija par plānoto IKT riska pārvaldības sistēmas turpmāko attīstību;

j) secinājumi, kas izriet no IKT riska pārvaldības sistēmas pārskatīšanas;

k) informācija par līdzšinēju pārskatīšanu, tajā skaitā:

i) līdzšinējas pārskatīšanas datumi;

ii) attiecīgā gadījumā – pēdējā ziņojumā noteikto korektīvo pasākumu īstenošanas stāvoklis;

iii) ja līdzšinējā pārskatīšanā ieteiktie korektīvie pasākumi ir izrādījušies neefektīvi vai ir radījuši neparedzamas problēmas – apraksts par to, kā šos korektīvos pasākumus varētu uzlabot, vai minēto neparedzēto problēmu apraksts;

l) ziņojuma sagatavošanā izmantotie informācijas avoti, ietverot visu turpmāk minēto:

i) attiecībā uz finanšu vienībām, kas nav mikrouzņēmumi, kā minēts Regulas (ES) 2022/2554 6. panta 6. punktā, – iekšējo revīziju rezultāti;

ii) atbilstības novērtējumu rezultāti;

iii) digitālās darbības noturības testēšanas rezultāti un – attiecīgā gadījumā – rezultāti, kas gūti IKT rīku, sistēmu un procesu padziļinātā testēšanā, kura veikta, pamatojoties uz draudu vadītu ielaušanās testēšanu (DVIT);

iv) ārējie avoti.

Šā punkta c) apakšpunkta nolūkos, ja pārskatīšana bija uzsākta, ievērojot uzraudzības norādījumus vai secinājumus, kas izriet no attiecīgajiem digitālās darbības noturības testēšanas vai revīzijas procesiem, ziņojumā iekļauj skaidras atsauces uz šādiem norādījumiem vai secinājumiem, lai varētu noteikt pārskatīšanas uzsākšanas iemeslu. Ja pārskatīšana uzsākta pēc tam, kad notikuši ar IKT saistīti incidenti, ziņojumā iekļauj visu ar IKT saistīto incidentu sarakstu kopā ar incidenta cēloņa analīzi.

Šā punkta f) apakšpunkta nolūkos aprakstā ietver analīzi par izmaiņu ietekmi uz finanšu vienības digitālās darbības noturības stratēģiju, uz finanšu vienības IKT iekšējo kontroles sistēmu un uz finanšu vienības IKT riska pārvaldības vadību.

III SADAĻA

VIENKĀRŠOTA IKT RISKA PĀRVALDĪBAS SISTĒMA FINANŠU VIENĪBĀM, KAS MINĒTAS REGULAS (ES) 2022/2554 16. PANTA 1. PUNKTĀ

I NODAĻA

Vienkāršota IKT riska pārvaldības sistēma

28. pants

Pārvaldība un organizācija

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētajām finanšu vienībām ir ieviesta iekšējā pārvaldības un kontroles sistēma, kas nodrošina efektīvu un prudenciālu IKT riska pārvaldību, lai sasniegtu augstu digitālās darbības noturības līmeni.

2. Šā panta 1. punktā minētās finanšu vienības savas vienkāršotās IKT riska pārvaldības sistēmas ietvaros nodrošina, ka to vadības struktūra:

a) uzņemas vispārējo atbildību par to, lai nodrošinātu, ka vienkāršotā IKT riska pārvaldības sistēma ļauj sasniegt finanšu vienības uzņēmējdarbības stratēģiju saskaņā ar attiecīgās finanšu vienības vēlmi uzņemties risku, un nodrošina, ka šajā kontekstā tiek ņemts vērā IKT risks;

b) nosaka visu ar IKT saistīto pienākumu uzdevumus un atbildību;

c) nosaka informācijas drošības mērķus un IKT prasības;

d) apstiprina, pārrauga un periodiski pārskata:

   i) finanšu vienības informācijas aktīvu klasifikāciju, kā noteikts šīs regulas 30. panta 1. punktā, galveno identificēto risku sarakstu un uzņēmējdarbības ietekmes analīzi un saistīto politiku;

   ii) finanšu vienības darbības nepārtrauktības plānus un reaģēšanas un seku novēršanas pasākumus, kas minēti Regulas (ES) 2022/2554 16. panta 1. punkta f) apakšpunktā;

e) piešķir un vismaz reizi gadā pārskata budžetu, kas nepieciešams, lai apmierinātu finanšu vienības digitālās darbības noturības vajadzības attiecībā uz visu veidu resursiem, tajā skaitā attiecīgajām IKT drošības izpratnes veidošanas programmām un digitālās darbības noturības mācībām, un IKT prasmēm visam personālam;

f) nosaka un īsteno politiku un pasākumus, kas ietverti šīs sadaļas I, II un III nodaļā, lai identificētu, novērtētu un pārvaldītu IKT risku, kam finanšu vienība ir pakļauta;

g) nosaka un īsteno procedūras, IKT protokolus un rīkus, kas nepieciešami, lai aizsargātu visus informācijas aktīvus un IKT aktīvus;

h) nodrošina, ka finanšu vienības darbinieki pastāvīgi atjaunina pietiekamas zināšanas un prasmes, kas ļauj saprast un novērtēt IKT risku un tā ietekmi uz finanšu vienības darbību, atbilstīgi pārvaldītajam IKT riskam;

i) nosaka ziņošanas kārtību, tajā skaitā tā ziņojuma biežumu, formu un saturu, kas izmantojams, lai ziņotu vadības struktūrai par informācijas drošību un digitālās darbības noturību.

3. Šā panta 1. punktā minētās finanšu vienības saskaņā ar Savienības un valsts nozaru tiesību aktiem var IKT riska pārvaldības prasību izpildes pārbaudes uzdevumus kā ārpakalpojumu uzticēt IKT pakalpojumu sniedzējiem, kas pieder vienai grupai, vai trešām personām, kas sniedz IKT pakalpojumus. Šādu ārpakalpojumu gadījumā finanšu vienības joprojām ir pilnībā atbildīgas par IKT riska pārvaldības prasību izpildes pārbaudi.

4. Šā panta 1. punktā minētās finanšu vienības nodrošina kontroles funkciju un iekšējās revīzijas funkciju pienācīgu nošķiršanu un neatkarību.

5. Šā panta 1. punktā minētās finanšu vienības nodrošina, ka revidenti veic to vienkāršotās IKT riska pārvaldības sistēmas iekšēju revīziju saskaņā ar finanšu vienību revīzijas plānu. Revidentiem ir pietiekamas zināšanas, prasmes un zinātība par IKT risku, un tie ir neatkarīgi. IKT revīzijas biežums un tajā galvenokārt pievērstā uzmanība ir samērīga ar finanšu vienības IKT riskam.

6. Pamatojoties uz 5. punktā minētās revīzijas rezultātu, 1. punktā minētās finanšu vienības nodrošina kritisko IKT revīzijas konstatējumu savlaicīgu pārbaudi un izlabošanu.

29. pants

Informācijas drošības politika un pasākumi

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības izstrādā, dokumentē un īsteno informācijas drošības politiku vienkāršotās IKT riska pārvaldības sistēmas kontekstā. Minētajā informācijas drošības politikā nosaka augsta līmeņa principus un noteikumus, lai aizsargātu datu un šo finanšu vienību sniegto pakalpojumu konfidencialitāti, integritāti, pieejamību un autentiskumu.

2. Pamatojoties uz 1. punktā minēto to informācijas drošības politiku, 1. punktā minētās finanšu vienības nosaka un īsteno IKT drošības pasākumus, lai mazinātu savu pakļautību IKT riskam, tajā skaitā riska mazināšanas pasākumus, ko īsteno trešās personas, kuras sniedz IKT pakalpojumus.

IKT drošības pasākumi ietver visus 30.–38. pantā minētos pasākumus.

30. pants

Informācijas aktīvu un IKT aktīvu klasifikācija

1. Kā daļu no vienkāršotās IKT riska pārvaldības sistēmas, kas minēta Regulas (ES) 2022/2554 16. panta 1. punkta a) apakšpunktā, minētā panta 1. punktā minētās finanšu vienības identificē, klasificē un dokumentē visas kritiskās vai svarīgās funkcijas, tās atbalstošos informācijas aktīvus un IKT aktīvus un to savstarpējo atkarību. Finanšu vienības pēc vajadzības pārskata minēto identifikāciju un klasifikāciju.

2. Šā panta 1. punktā minētās finanšu vienības identificē visas kritiski svarīgās vai svarīgās funkcijas, ko atbalsta trešās personas, kuras sniedz IKT pakalpojumus.

31. pants

IKT riska pārvaldība

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības savā vienkāršotajā IKT riska pārvaldības sistēmā iekļauj visus no šiem elementiem:

a) riska tolerances līmeņa noteikšana IKT riskam saskaņā ar finanšu vienības vēlmi uzņemties risku;

b) to IKT risku identifikācija un novērtējums, kuram finanšu vienība ir pakļauta;

c) riska mazināšanas stratēģiju noteikšana vismaz tiem IKT riskiem, kas neiekļaujas finanšu vienības riska tolerances līmenī;

d) c) apakšpunktā minēto riska mazināšanas stratēģiju efektivitātes uzraudzība;

e) jebkuru tādu IKT un informācijas drošības risku identifikācija un novērtējums, kuri izriet no jebkurām nozīmīgām IKT sistēmas vai IKT pakalpojumu, procesu vai procedūru izmaiņām un no IKT drošības testēšanas rezultātiem un pēc jebkura būtiska ar IKT saistīta incidenta.

2. Šā panta 1. punktā minētās finanšu vienības periodiski veic un dokumentē IKT riska novērtējumu atbilstīgi finanšu vienību IKT riska profilam.

3. Šā panta 1. punktā minētās finanšu vienības pastāvīgi uzrauga draudus un ievainojamību, kas ir būtiski attiecībā uz to kritiski svarīgajām vai svarīgajām funkcijām un informācijas aktīviem un IKT aktīviem, un regulāri pārskata riska scenārijus, kas ietekmē minētās kritiski svarīgās vai svarīgās funkcijas.

4. Šā panta 1. punktā minētās finanšu vienības nosaka brīdināšanas mehānismu robežvērtības un kritērijus, atbilstīgi kuriem tiek ierosināti un uzsākti ar IKT saistīto incidentu reaģēšanas procesi.

32. pants

Fiziskā un vides drošība

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības identificē un īsteno fiziskās drošības pasākumus, kas izstrādāti, pamatojoties uz kiberdraudu vidi un saskaņā ar šīs regulas 30. panta 1. punktā minēto klasifikāciju, IKT aktīvu vispārējo riska profilu un pieejamiem informācijas aktīviem.

2. Šā panta 1. punktā minētie pasākumi aizsargā finanšu vienību telpas un attiecīgā gadījumā finanšu vienību datu centrus, kur atrodas IKT aktīvi un informācijas aktīvi, no neatļautas piekļuves, uzbrukumiem un negadījumiem un no vides draudiem un apdraudējumiem.

3. Aizsardzība pret vides draudiem un apdraudējumiem ir samērīga ar attiecīgo telpu un attiecīgā gadījumā datu centru svarīgumu un tajās notiekošo darbību vai esošo IKT sistēmu kritiskumu.

II NODAĻA

IKT riska ietekmes mazināšanas sistēmu, protokolu un rīku papildu elementi

33. pants

Piekļuves kontrole

Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības izstrādā, dokumentē un īsteno procedūras loģiskās un fiziskās piekļuves kontrolei un īsteno, uzrauga un periodiski pārskata šīs procedūras. Minētās procedūras ietver šādus loģiskās un fiziskās piekļuves kontroles elementus:

a) tiesības attiecībā uz piekļuvi informācijas aktīviem, IKT aktīviem un to atbalstītajām funkcijām, un finanšu vienības darbības kritiskajām vietām tiek pārvaldītas saskaņā ar principiem "vajadzība zināt", "vajadzība izmantot" un mazāko tiesību principu, arī attiecībā uz attālu un ārkārtas piekļuvi;

b) lietotāju pārskatatbildība, kas nodrošina, ka lietotājus var identificēt attiecībā uz IKT sistēmās veiktajām darbībām;

c) kontu pārvaldības procedūras, lai piešķirtu, mainītu vai atsauktu piekļuves tiesības lietotāju un vispārējiem kontiem, tajā skaitā vispārējiem administratoru kontiem;

d) autentifikācijas metodes, kas ir samērīgas ar 30. panta 1. punktā minēto klasifikāciju un IKT aktīvu vispārējo riska profilu un ir balstītas uz paraugpraksi;

e) piekļuves tiesības tiek periodiski pārskatītas un atsauktas, kad tās vairs nav vajadzīgas.

Šā punkta c) apakšpunkta nolūkos finanšu vienība piešķir privileģētu, ārkārtas un administratora piekļuvi pēc principa "vajadzība izmantot" vai uz *ad hoc* pamata attiecībā uz visām IKT sistēmām, un to reģistrē žurnālā saskaņā ar 34. panta pirmās daļas f) punktu.

Šā punkta d) apakšpunkta nolūkos finanšu vienības izmanto stingras, uz paraugpraksi balstītas autentifikācijas metodes attiecībā uz attālu piekļuvi finanšu vienību tīklam, privileģētu piekļuvi un piekļuvi IKT aktīviem, kas atbalsta kritiski svarīgas vai svarīgas funkcijas, kuras ir publiski pieejamas.

34. pants

IKT darbību drošība

Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības savu sistēmu, protokolu un rīku ietvaros un attiecībā uz visiem IKT aktīviem:

a) uzrauga un pārvalda visu IKT aktīvu aprites ciklu;

b) attiecīgā gadījumā uzrauga, vai IKT aktīvus atbalsta finanšu vienību trešās personas, kas sniedz IKT pakalpojumus;

c) identificē savu IKT aktīvu jaudas prasības un pasākumus, lai saglabātu un uzlabotu IKT sistēmu pieejamību un efektivitāti un novērstu IKT jaudas trūkumu, pirms tas rodas;

d) veic automatizētu ievainojamības izvērtēšanu un IKT aktīvu novērtējumus atbilstīgi to klasifikācijai, kas minēta 30. panta 1. punktā, un IKT aktīva vispārējam riska profilam un izmanto ielāpus, lai risinātu identificēto ievainojamību;

e) pārvalda riskus, kas saistīti ar novecojušiem, neatbalstītiem vai mantotiem IKT aktīviem;

f) reģistrē notikumus, kas saistīti ar loģiskās un fiziskās piekļuves kontroli, IKT darbībām, tajā skaitā sistēmu un tīklu datplūsmas darbībām, un IKT izmaiņu pārvaldību;

g) identificē un īsteno pasākumus, lai uzraudzītu un analizētu informāciju par anomālām darbībām un uzvedību attiecībā uz kritiski svarīgām vai svarīgām IKT darbībām;

h) īsteno pasākumus, lai uzraudzītu būtisko un aktuālo informāciju par kiberdraudiem;

i) īsteno pasākumus, lai apzinātu iespējamas informācijas noplūdes, ļaunprātīgus kodus un citus drošības apdraudējumus, un publiski zināmu ievainojamību attiecībā uz programmatūru un aparatūru, un pārbauda, vai nav atbilstošu jaunu drošības atjauninājumu.

Šā punkta f) apakšpunkta nolūkos finanšu vienības pielāgo žurnālu detalizācijas līmeni to mērķim un IKT aktīva, kas sagatavo šos žurnālus, izmantojumam.

35. pants

Datu, sistēmu un tīkla drošība

Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības kā daļu no savām sistēmām, protokoliem un rīkiem izstrādā un īsteno aizsardzības pasākumus, kas nodrošina tīklu aizsardzību pret ielaušanos un datu ļaunprātīgu izmantošanu un kas saglabā datu pieejamību, autentiskumu, integritāti un konfidencialitāti. Konkrētāk, finanšu vienības, ņemot vērā šīs regulas 30. panta 1. punktā minēto klasifikāciju, nosaka:

a) pasākumu identifikāciju un īstenošanu, lai aizsargātu datus, kad tie tiek izmantoti, tiek nosūtīti vai tiek glabāti;

b) drošības pasākumu identifikāciju un īstenošanu attiecībā uz tādas programmatūras, datu nesēju, sistēmu un galapunkta ierīču izmantošanu, kuras nosūta un glabā finanšu vienības datus;

c) pasākumu identifikāciju un īstenošanu, lai novērstu un atklātu neatļautu pieslēgšanos finanšu vienības tīklam un aizsargātu tīkla datplūsmu starp finanšu vienības iekšējiem tīkliem un internetu un citiem ārējiem pieslēgumiem;

d) pasākumu identifikāciju un īstenošanu, lai nodrošinātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, kad notiek nosūtīšana tīklā;

e) procesu to datu drošai dzēšanai, kas tiek turēti telpās vai tiek glabāti ārēji un ko finanšu vienībai vairs nav nepieciešams vākt vai glabāt;

f) procesu, lai droši utilizētu vai izņemtu no ekspluatācijas telpās esošās datu glabāšanas ierīces vai datu glabāšanas ierīces, kas tiek glabātas ārēji un kas satur konfidenciālu informāciju;

g) pasākumu identifikāciju un īstenošanu, lai nodrošinātu, ka tāldarbs un privātu galapunkta ierīču izmantošana nelabvēlīgi neietekmē finanšu vienības spēju veikt tās kritiski svarīgās darbības pienācīgā, savlaicīgā un drošā veidā.

36. pants

IKT drošības testēšana

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības izstrādā un īsteno IKT drošības testēšanas plānu, lai validētu to savu IKT drošības pasākumu efektivitāti, kuri izstrādāti saskaņā ar šīs regulas 33., 34., 35., 37. un 38. pantu. Finanšu vienības nodrošina, ka minētajā plānā ir ņemti vērā draudi un ievainojamība, kas identificēta šīs regulas 31. panta minētās vienkāršotās IKT riska pārvaldības sistēmas ietvaros.

2. Šā panta 1. punktā minētās finanšu vienības pārskata, novērtē un testē IKT drošības pasākumus, ņemot vērā finanšu vienības IKT aktīvu vispārējo riska profilu.

3. Šā panta 1. punktā minētās finanšu vienības uzrauga un izvērtē drošības testu rezultātus un bez nepamatotas kavēšanās attiecīgi atjaunina drošības pasākumus tādu IKT sistēmu gadījumā, kas atbalsta kritiski svarīgas vai svarīgas funkcijas.

37. pants

IKT sistēmu iegāde, izstrāde un uzturēšana

Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības attiecīgā gadījumā izstrādā un īsteno procedūru, kas reglamentē IKT sistēmu iegādi, izstrādi un uzturēšanu, ievērojot uz risku balstītu pieeju. Minētā procedūra:

a) nodrošina, ka pirms jebkuras IKT sistēmu iegādes vai izstrādes attiecīgā uzņēmējdarbības funkcija skaidri nosaka un apstiprina funkcionālās un nefunkcionālās prasības, tajā skaitā informācijas drošības prasības;

b) nodrošina IKT sistēmu testēšanu un apstiprināšanu pirms to pirmreizējās izmantošanas un pirms izmaiņu ieviešanas ražošanas vidē;

c) nosaka pasākumus, lai mazinātu IKT sistēmu nejaušas pārveides vai tīšu manipulāciju ar tām risku, kad notiek izstrāde un ieviešana ražošanas vidē.

38. pants

IKT projektu un izmaiņu pārvaldība

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības izstrādā, dokumentē un īsteno IKT projektu pārvaldības procedūru un nosaka uzdevumus un atbildību par tās īstenošanu. Minētā procedūra aptver visus IKT projektu posmus no to uzsākšanas līdz slēgšanai.

2. Šā panta 1. punktā minētās finanšu vienības izstrādā, dokumentē un īsteno IKT izmaiņu pārvaldības procedūru, lai nodrošinātu, ka visas IKT sistēmu izmaiņas tiek reģistrētas, testētas, novērtētas, īstenotas un verificētas kontrolētā veidā un ievērojot pienācīgus aizsardzības pasākumus, lai saglabātu finanšu vienības digitālās darbības noturību.

III NODAĻA

IKT darbības nepārtrauktības pārvaldība

39. pants

IKT darbības nepārtrauktības plāna elementi

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības izstrādā savus IKT darbības nepārtrauktības plānus, ņemot vērā rezultātus, kas gūti analīzē par to pakļautību nopietnu uzņēmējdarbības traucējumu riskam un šādu traucējumu potenciālo ietekmi, un scenārijus, kam varētu būt pakļauti to IKT aktīvi, kuri atbalsta kritiski svarīgas vai svarīgas funkcijas, tajā skaitā kiberuzbrukuma scenāriju.

2. Šā panta 1. punktā minētie IKT darbības nepārtrauktības plāni:

a) tiek apstiprināti finanšu vienības vadības struktūrā;

b) tiek dokumentēti un ir ātri pieejami ārkārtas vai krīzes gadījumā;

c) paredz pietiekamus resursus to izpildei;

d) nosaka plānotos seku novēršanas līmeņus un termiņus funkciju un galveno iekšējo un ārējo atkarību, tajā skaitā trešo personu, kas sniedz IKT pakalpojumus, atgūšanai un atjaunošanai;

e) paredz nosacījumus, kuriem izpildoties, var aktivizēt IKT darbības nepārtrauktības plānus, un nosaka, kādas darbības ir jāveic, lai nodrošinātu finanšu vienību IKT aktīvu, kas atbalsta kritiski svarīgas vai svarīgas funkcijas, pieejamību, nepārtrauktību un atgūšanu;

f) nosaka atjaunošanas un atgūšanas pasākumus kritiski svarīgām vai svarīgām uzņēmējdarbības funkcijām, atbalsta procesiem, informācijas aktīviem un to savstarpējai atkarībai, lai izvairītos no nelabvēlīgas ietekmes uz finanšu vienību darbību;

g) paredz rezerves kopiju veidošanas procedūras un pasākumus, kas nosaka to datu tvērumu, kuriem jāveido rezerves kopijas, un rezerves kopiju veidošanas minimālo biežumu, pamatojoties uz šos datus izmantojošās funkcijas svarīgumu;

h) ņem vērā alternatīvas iespējas, ja atgūšana īstermiņā nav iespējama izmaksu, riska, loģistikas vai neparedzētu apstākļu dēļ;

i) nosaka iekšējās un ārējās saziņas kārtību, tajā skaitā eskalācijas plānus;

j) tiek atjaunināti atbilstīgi atziņām, kas gūtas no incidentiem, testiem, jauniem riskiem un apzinātajiem draudiem, mainītiem atgūšanas mērķiem, būtiskām izmaiņām finanšu vienības organizācijā un IKT aktīvos, kas atbalsta kritiski svarīgas vai uzņēmējdarbības funkcijas.

Šā punkta f) apakšpunkta nolūkos minētajā punktā paredzētie pasākumi paredz kritisku trešo personu, kas sniedz pakalpojumus, atteiču mazināšanu.

40. pants

Darbības nepārtrauktības plānu testēšana

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības testē savus šīs regulas 39. pantā minētos darbības nepārtrauktības plānus, tajā skaitā minētajā pantā norādītos scenārijus, vismaz reizi gadā rezerves kopiju veidošanas un atjaunošanas procedūrām vai ikreiz, kad notiek būtiskas izmaiņas darbības nepārtrauktības plānā.

2. Šā panta 1. punktā minētajā darbības nepārtrauktības plānu testēšanā pierāda, ka minētajā punktā norādītās finanšu vienības spēj uzturēt savu uzņēmumu dzīvotspēju, līdz tiek atjaunotas kritiski svarīgās darbības, un identificē visus trūkumus minētajos plānos.

3. Šļā panta 1. punktā minētās finanšu vienības dokumentē darbības nepārtrauktības plānu testēšanas rezultātus, un visas no minētās testēšanas izrietošās nepilnības analizē, risina un paziņo vadības struktūrai.

IV NODAĻA

Ziņojums par vienkāršotās IKT riska pārvaldības sistēmas pārskatīšanu

41. pants

Ziņojuma par vienkāršotās IKT riska pārvaldības sistēmas pārskatīšanu formāts un saturs

1. Regulas (ES) 2022/2554 16. panta 1. punktā minētās finanšu vienības iesniedz minētā panta 2. punktā norādīto ziņojumu par IKT riska pārvaldības sistēmas pārskatīšanu elektroniskā formātā, kurā ir iespējams veikt meklēšanu.

2. Šā panta 1. punktā minētajā ziņojumā ietver visu turpmāk minēto informāciju:

a) ievada iedaļa, kurā ietver:

   i) aprakstu par ziņojuma kontekstu – finanšu vienības pakalpojumu, pasākumu un darbību veidu, mērogu un sarežģītību, finanšu vienības organizāciju, identificētajām kritiskajām funkcijām, stratēģiju, būtiskiem notiekošiem projektiem vai darbībām, un attiecībām, un finanšu vienības atkarību no vietējiem vai ārpakalpojumu sniedzējiem uzticētiem IKT pakalpojumiem un sistēmām vai ietekmi, kāda šādu sistēmu pilnīgai zaudēšanai vai būtiskam darbības pasliktinājumam būtu uz kritiskajām vai svarīgajām funkcijām un tirgus efektivitāti;

   ii) izpildvaras līmeņa kopsavilkumu par apzināto pašreizējo un īstermiņa IKT risku, draudu vidi, novērtēto tās kontroļu efektivitāti un finanšu vienības drošības stāvokli;

   iii) informāciju par jomu, par kuru tiek ziņots;

   iv) kopsavilkumu par nozīmīgām IKT riska pārvaldības sistēmas izmaiņām kopš iepriekšējā iesniegtā ziņojuma;

   v) kopsavilkumu un aprakstu par būtisku vienkāršotās IKT riska pārvaldības sistēmas izmaiņu ietekmi kopš iepriekšējā ziņojuma;

b) attiecīgā gadījumā – datums, kurā finanšu vienības vadības struktūra apstiprinājusi ziņojumu;

c) pārskatīšanas iemeslu apraksts, ietverot:

   i) ja pārskatīšana sākta pēc uzraudzības norādījumiem – pierādījumus par šādiem norādījumiem;

   ii) ja pārskatīšana sākta pēc tam, kad notikuši ar IKT saistīti incidenti, – visu šo ar IKT saistīto incidentu sarakstu kopā ar saistīto cēloņu analīzi;

d) pārskata perioda sākuma un beigu datums;

e) par pārskatīšanu atbildīgā persona;

f) konstatējumu kopsavilkums un pašnovērtējums par IKT riska pārvaldības sistēmā apzināto vājo vietu, trūkumu un nepilnību smagumu par pārskata periodu, iekļaujot sīku to analīzi;

g) noteiktie izlabošanas pasākumi vienkāršotās IKT riska pārvaldības sistēmas vājo vietu, trūkumu un nepilnību risināšanai un paredzamais datums šo pasākumu īstenošanai, tajā skaitā turpmākā rīcība pēc iepriekšējos ziņojumos identificētajām vājajām vietām, trūkumiem un nepilnībām, ja šīs vājās vietas, trūkumi un nepilnības vēl nav novērstas;

h) vispārēji secinājumi par vienkāršotās IKT riska pārvaldības sistēmas pārskatīšanu, tajā skaitā jebkāda turpmāk plānotā attīstība.

IV SADAĻA

NOBEIGUMA NOTEIKUMI

42. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2024. gada 13. martā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN