Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1190

18.6.2025.

KOMISIJAS DELEĢĒTĀ REGULA (ES) 2025/1190

(2025. gada 13. februāris),

ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem, kuros precizēti kritēriji, ko izmanto, lai identificētu finanšu vienības, kurām ir pienākums veikt draudu vadītu ielaušanās testēšanu, prasības un standarti, kas reglamentē iekšējo testētāju izmantošanu, prasības attiecībā uz darbības jomu, testēšanas metodiku un pieeju katram testēšanas posmam, rezultātiem, slēgšanas un kļūdu novēršanas posmiem, kā arī uzraudzības un citas attiecīgas sadarbības veids, kas nepieciešams, lai īstenotu DVIT un veicinātu savstarpēju atzīšanu

(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 nozares 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 26. panta 11. punkta ceturto daļu,

tā kā:

(1) Šī regula ir izstrādāta saskaņā ar *TIBER-EU* sistēmu un līdzinās *TIBER-EU* aprakstītajai draudu vadītas ielaušanās testēšanas (DVIT) metodikai, procesam un struktūrai. Finanšu vienības, uz kurām attiecas DVIT, var atsaukties uz *TIBER-EU* sistēmu vai kādu no tās valsts īstenošanas pasākumiem un to piemērot, ciktāl minētā sistēma vai īstenošanas pasākums atbilst Regulas (ES) 2022/2554 26. un 27. pantā un šajā regulā noteiktajām prasībām. Tādas vienotas publiskās iestādes izraudzīšanai finanšu nozarē, kas valsts līmenī ir atbildīga par jautājumiem, kuri saistīti ar DVIT, saskaņā ar Regulas (ES) 2022/2554 26. panta 9. punktu, nebūtu jāskar kompetento iestāžu kompetence, kas Savienības līmenī uzticēta konkrētu finanšu vienību uzraudzībai saskaņā ar minētās regulas 46. pantu, piemēram, Eiropas Centrālajai bankai attiecībā uz nozīmīgām kredītiestādēm, kuras uzskatāmas par kompetentām ar DVIT saistītos jautājumos. Ja tikai daži no uzdevumiem, kas saistīti ar DVIT, ir deleģēti citai valsts iestādei finanšu nozarē saskaņā ar Regulas (ES) 2022/2554 26. panta 10. punktu, minētās regulas 46. pantā minētās finanšu vienības kompetentajai iestādei arī turpmāk vajadzētu būt iestādei, kas veic ar DVIT saistītos uzdevumus, kuri nav deleģēti.

(2) Ņemot vērā DVIT sarežģītību un ar to saistītos riskus, tās izmantošana būtu jāattiecina tikai uz tām finanšu vienībām, kurām to veikt ir pamatoti. Tādējādi iestādēm, kas atbild par DVIT jautājumiem (DVIT iestādēm Savienības vai valsts līmenī), no DVIT darbības jomas būtu jāizslēdz tās finanšu vienības, kuras darbojas finanšu pamatpakalpojumu apakšnozarēs un kurām veikt DVIT nav pamatoti. Tas nozīmē, ka kredītiestādes, maksājumu un elektroniskās naudas iestādes, centrālos vērtspapīru depozitārijus, centrālos darījumu partnerus, tirdzniecības vietas, apdrošināšanas un pārapdrošināšanas sabiedrības, pat ja tās atbilst kvantitatīvajiem kritērijiem, varētu atbrīvot no DVIT prasības, ņemot vērā to IKT riska profila un gatavības līmeņa vispārēju novērtējumu, ietekmi uz finanšu nozari un ar to saistītās bažas par finanšu stabilitāti.

(3) DVIT iestādēm, ņemot vērā IKT riska profila un gatavības līmeņa vispārēju novērtējumu, ietekmi uz finanšu nozari un ar to saistītās bažas par finanšu stabilitāti, būtu jānovērtē, vai DVIT būtu jāattiecina uz jebkāda veida finanšu vienību, kas nav kredītiestāde, maksājumu iestāde, elektroniskās naudas iestāde, centrālais darījumu partneris, centrālais vērtspapīru depozitārijs, tirdzniecības vieta, apdrošināšanas un pārapdrošināšanas sabiedrība. Novērtējumam par to, vai šādas finanšu vienības atbilst minētajiem kvalitatīvajiem kritērijiem, vajadzētu būt vērstam uz to, lai identificētu finanšu vienības, kurām DVIT ir piemērota, izmantojot starpnozaru un objektīvus rādītājus. Tajā pašā laikā novērtējumā par to, vai finanšu vienība atbilst minētajiem kvalitatīvajiem kritērijiem, būtu no vienībām, uz kurām attiecas DVIT, jāizraugās vienības, kurām testēšanu veikt ir pamatoti. Tas, vai finanšu vienība atbilst minētajiem

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

kvalitatīvajiem kritērijiem, būtu jānovērtē arī, ņemot vērā jaunu tirgu attīstību un jaunu tirgus dalībnieku, tostarp kriptoaktīvu pakalpojumu sniedzēju, kas saņēmuši atļauju saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2023/1114 ([2]) 59. pantu, pieaugošo nozīmi finanšu nozarē nākotnē.

(4) Finanšu vienībām var būt viens un tas pats IKT pakalpojumu sniedzējs, kurš pieder vienai grupai, vai tās var piederēt vienai un tai pašai grupai un paļauties uz kopīgu IKT sistēmu izmantošanu. Šādā gadījumā novērtējumā par to, vai uz finanšu vienību būtu jāattiecina DVIT un vai DVIT būtu jāveic vienības vai grupas līmenī (ar kopīgas DVIT starpniecību), ir svarīgi, lai DVIT iestādes ņemtu vērā minētās finanšu vienības struktūru un sistēmisko raksturu vai nozīmi finanšu nozarē valsts vai Savienības līmenī.

(5) Nolūkā līdzināties *TIBER-ES* sistēmai, ir nepieciešams, lai testēšanas metodika paredzētu šādu galveno dalībnieku iesaisti: finanšu vienība ar kontroles komandu (kas līdzinās *TIBER-EU* "kontroles komandai") un zilo komandu (kas līdzinās *TIBER-EU* "zilajai komandai") un DVIT iestāde DVIT kiberkomandas veidā (kas līdzinās *TIBER-EU* "*TIBER* kiberkomandām"), draudu izlūkdatu sniedzējs un testētāji (kur testētāji līdzinās *TIBER-EU* "sarkanās komandas nodrošinātājam").

(6) Lai nodrošinātu, ka DVIT gūst labumu no pieredzes, kas gūta saistībā ar *TIBER-EU* īstenošanu, un lai samazinātu riskus, kuri saistīti ar DVIT veikšanu, būtu jānodrošina, ka DVIT kiberkomandu, kas jāizveido DVIT iestāžu līmenī, pienākumi pēc iespējas sakrīt ar *TIBER-EU* kiberkomandu pienākumiem. Tādējādi DVIT kiberkomandām vajadzētu būt testu pārvaldniekiem, kas ir atbildīgi par atsevišķu DVIT pārraudzību un atsevišķu testu plānošanu un koordinēšanu. DVIT kiberkomandām būtu jādarbojas kā vienotam kontaktpunktam ar testiem saistītai saziņai, kura vērsta uz iekšējām un ārējām ieinteresētajām personām, atsauksmju un iepriekš veiktos testos gūto atziņu apkopošanai un apstrādei, kā arī atbalstam finanšu vienībām, kurām tiek veikta DVIT.

(7) Nolūkā līdzināties *TIBER-ES* sistēmas metodikai, testu pārvaldniekiem vajadzētu būt prasmēm un spējām, kas nepieciešamas, lai sniegtu konsultācijas un apstrīdētu testētāju priekšlikumus. Pieredze saistībā ar *TIBER-EU* sistēmu ir pierādījusi, ka ir vērtīgi uz katru testu norīkot komandu ar vismaz diviem testu pārvaldniekiem. Nolūkā atspoguļot to, ka DVIT tiek izmantota, lai veicinātu mācīšanās pieredzi, un aizsargāt testu konfidencialitāti, DVIT iestādes, ja vien tās nesaskaras ar resursu vai speciālo zināšanu problēmām, tiek stingri mudinātas apsvērt, lai DVIT laikā testu pārvaldniekiem nebūtu jāveic uzraudzības darbības tai pašai finanšu vienībai, kurai veic DVIT.

(8) Lai nodrošinātu saskaņotību ar *TIBER-EU* sistēmu, ir svarīgi, lai DVIT iestāde cieši sekotu līdzi testēšanai katrā tās posmā. Ņemot vērā testēšanas raksturu un ar to saistītos riskus, ir būtiski, lai DVIT iestāde būtu iesaistīta katrā konkrētajā testēšanas posmā. Jo īpaši būtu jāapspriežas ar DVIT iestādi, un tai būtu jāapstiprina tie finanšu vienību novērtējumi vai lēmumi, kas, no vienas puses, var iespaidot testa rezultativitāti un, no otras puses, ietekmēt ar testu saistītos riskus. Galvenie posmi, kuros ir vajadzīga īpaša DVIT iestādes iesaistīšanās, ietver konkrētu testēšanas pamatdokumentu apstiprināšanu, draudu izlūkdatu sniedzēju un testētāju atlasi un riska pārvaldības pasākumus. DVIT iestāžu iesaistei – jo īpaši attiecībā uz apstiprināšanu – nevajadzētu radīt pārmērīgu slogu minētajām iestādēm, un tāpēc tai būtu jāattiecas tikai uz tiem dokumentiem un lēmumiem, kuri tieši ietekmē DVIT veikšanu. Aktīvi piedaloties katrā testēšanas posmā, DVIT iestādes var rezultatīvi novērtēt finanšu vienību atbilstību attiecīgajām prasībām, un tam būtu jāļauj minētajām iestādēm izdot apliecinājumus saskaņā ar Regulas (ES) 2022/2554 26. panta 7. punktu.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2023/1114 (2023. gada 31. maijs) par kriptoaktīvu tirgiem un ar ko groza Regulas (ES) Nr. 1093/2010 un (ES) Nr. 1095/2010 un Direktīvas 2013/36/ES un (ES) 2019/1937 (OV L 150, 9.6.2023., 40. lpp., ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) DVIT slepenība ir ārkārtīgi svarīga, lai nodrošinātu, ka testēšanas apstākļi ir reālistiski. Šā iemesla dēļ testēšanai vajadzētu būt slēptai, un būtu jāveic piesardzības pasākumi, kas paredzēti, lai saglabātu DVIT konfidencialitāti, tostarp izvēloties kodētus nosaukumus, kuri būtu jāizstrādā, lai novērstu, ka trešās personas var identificēt DVIT. Ja darbinieki, kas ir atbildīgi par finanšu vienības drošību, ir informēti par plānotu vai notiekošu DVIT, ir iespējams, ka viņi ievēros lielāku uzmanību un piesardzību nekā parastos darba apstākļos, tādējādi testēšanas rezultāti var mainīties. Tāpēc, lai *inter alia* nodrošinātu testa slepenību gadījumā, ja zilās komandas dalībnieks ir konstatējis, ka notiek testēšana, finanšu vienības darbinieki ārpus kontroles komandas par jebkādu plānotu vai notiekošu DVIT būtu jāinformē tikai tad, ja ir pārliecinoši iemesli un ja iepriekš ir saņemta testu pārvaldnieku piekrišana.

(10) Kā liecina pieredze, kas *TIBER-EU* sistēmas ietvaros gūta attiecībā uz "kontroles komandu", lai droši veiktu DVIT, ir obligāti jāizraugās pienācīgs kontroles komandas vadītājs. Kontroles komandas vadītājam vajadzētu būt nepieciešamajām pilnvarām finanšu vienībā vadīt visus testēšanas aspektus, neapdraudot tās konfidencialitāti. Tā paša iemesla dēļ kontroles komandas locekļiem vajadzētu būt padziļinātām zināšanām par finanšu vienību, kontroles komandas vadītāja amatu un stratēģisko pozicionēšanu, kā arī nepieciešamajam amata stāžam un piekļuvei valdei. Lai samazinātu risku, ka var tikt apdraudēta DVIT, kontroles komandai vajadzētu būt pēc iespējas mazākai.

(11) Pastāv ar DVIT saistīti raksturīgi riska elementi, jo kritiski svarīgās funkcijas izstrādes vidē tiek testētas reāllaikā, kas var izraisīt pakalpojuma atteikuma incidentus, negaidītas sistēmas avārijas, kaitējumu kritiski svarīgām izstrādes sistēmām reāllaikā vai datu zudumu, pārveidošanu vai izpaušanu. Šie riski liecina, ka ir vajadzīgi stingri riska pārvaldības pasākumi. Nolūkā nodrošināt, ka DVIT visā testēšanas laikā tiek veikta kontrolēti, ir ļoti svarīgi, lai finanšu vienības visos posmos apzinātos konkrētos riskus, kas rodas DVIT gaitā, un lai šie riski tiktu mazināti. Šajā sakarā, neskarot finanšu vienības iekšējos procesus un kontroles komandas vadītājam jau uzticēto atbildību un deleģējumus, varētu būt piemēroti sniegt informāciju par DVIT riska pārvaldības pasākumiem vai – īpašos gadījumos – pašai finanšu vienības vadības struktūrai apstiprināt minētos riska pārvaldības pasākumus. Nolūkā sniegt rezultatīvus un augsti kvalificētus profesionālos pakalpojumus un samazināt minētos riskus ir arī svarīgi, lai testētājiem un draudu izlūkdatu sniedzējiem (kopā – DVIT pakalpojumu sniedzējiem) būtu visaugstākais prasmju, speciālo zināšanu un atbilstošas pieredzes līmenis draudu izlūkdatu un DVIT jomā finanšu pakalpojumu nozarē.

(12) Konvencionālie ielaušanās testi sniedz detalizētu un noderīgu novērtējumu par tehnisko un konfigurācijas ievainojamību, bieži vien atsevišķi par vienu sistēmu vai vidi, bet atšķirībā no izlūkdatu vadīta sarkanās komandas testa nenovērtē pilnīgu scenāriju, kurā mērķtiecīgs uzbrukums ir vērsts pret visu vienību, tostarp tās cilvēku, procesu un tehnoloģiju kopējo spektru. Tāpēc DVIT pakalpojumu sniedzēju atlases procesā finanšu vienībām būtu jānodrošina, ka šiem pakalpojumu sniedzējiem ir nepieciešamās prasmes veikt izlūkdatu vadītus sarkanās komandas testus, nevis tikai ielaušanās testus. Tādēļ ir jāparedz visaptveroši kritēriji gan iekšējiem, gan ārējiem testētājiem, kā arī draudu izlūkdatu sniedzējiem, kas vienmēr ir ārēji. Ja DVIT pakalpojumu sniedzēji ir no viena un tā paša uzņēmuma, DVIT norīkotie darbinieki būtu pienācīgi jānodala.

(13) Var būt izņēmuma apstākļi, kad finanšu vienības nevar noslēgt līgumus ar DVIT pakalpojumu sniedzējiem, kas atbilst visaptverošajiem kritērijiem. Tāpēc finanšu vienībām, sniedzot pierādījumus par šādu draudu izlūkdatu sniedzēju nepieejamību, būtu jāļauj iesaistīt personas, kas neatbilst visiem visaptverošajiem kritērijiem, ar noteikumu, ka tās pienācīgi mazina jebkādus izrietošos papildu riskus un ka DVIT iestāde novērtē visus minētos kritērijus.

(14) Lai veiktu visefektīvāko un drošāko testu, būtu jāprecizē visu DVIT procesā iesaistīto pušu loma, ja DVIT ir iesaistītas vairākas finanšu vienības un vairākas DVIT iestādes. Apvienotas testēšanas nolūkos ir jānosaka īpašas prasības, lai precizētu izraudzītās finanšu vienības lomu, proti, ka tai vajadzētu būt atbildīgai par visas nepieciešamās dokumentācijas sniegšanu vadošajai DVIT iestādei un testēšanas procesa uzraudzību. Izraudzītajai finanšu vienībai vajadzētu būt atbildīgai arī par riska pārvaldības novērtējuma kopīgajiem aspektiem. Katras tās finanšu vienības pienākumiem, kura piedalās apvienotās DVIT procesā, vajadzētu saglabāties neskartiem neatkarīgi no izraudzītās finanšu vienības lomas. Tas pats princips būtu jāpiemēro kopīgām DVIT.

(15) Kā liecina *TIBER-EU* sistēmas īstenošanas pieredze, visefektīvākais veids, kā nodrošināt pienācīgu testēšanas veikšanu, ir klātienes vai virtuālas sanāksmes, kurās piedalās visas attiecīgās ieinteresētās personas (finanšu vienības, iestādes, testētāji un draudu izlūkdatu sniedzēji). Tāpēc klātienes un virtuālas sanāksmes būtu jārīko dažādos procesa posmos, jo īpaši sagatavošanas posmā, kad DVIT tiek uzsākta, un lai pabeigtu tās darbības jomas noteikšanu, testēšanas posmā, lai pabeigtu draudu izlūkdatu ziņojuma un sarkanās komandas testēšanas plāna izstrādi un sniegtu iknedēļas atjauninājumus, un slēgšanas posmā – testētāju un zilās komandas darbību atkārtošanai, purpursarkanās komandas izmatošanai un lai apmainītos ar atsauksmēm par DVIT.

(16) Lai nodrošinātu DVIT netraucētu veikšanu, DVIT iestādei savas gaidas attiecībā uz testēšanu būtu skaidri jāizklāsta finanšu vienībai. Šajā sakarā testu pārvaldniekiem būtu jānodrošina, ka finanšu vienībā tiek izveidota atbilstoša informācijas plūsma ar kontroles komandu, kā arī ar DVIT pakalpojumu sniedzējiem.

(17) Finanšu vienībai būtu jāatlasa kritiski svarīgās vai svarīgās funkcijas, kuras būs DVIT darbības jomā. Atlasot minētās funkcijas, finanšu vienībai būtu jābalstās uz dažādiem kritērijiem, kas saistīti ar katras funkcijas nozīmīgumu pašai finanšu vienībai un finanšu nozarei Savienības un valsts līmenī ne tikai ekonomiskā ziņā, bet arī ņemot vērā funkcijas simbolisko vai politisko statusu. Lai veicinātu netraucētu pāreju uz draudu izlūkdatu vākšanas posmu, kontroles komandai darbības jomas noteikšanas procesā neiesaistītajiem testētājiem un draudu izlūkdatu sniedzējam būtu jāsniedz detalizēta informācija par saskaņoto darbības jomu.

(18) Lai testētājiem sniegtu tāda reālistiska uzbrukuma simulēšanai nepieciešamo informāciju, kas ikdienā var notikt finanšu vienības kritiski svarīgo vai svarīgo funkciju pamatā esošajām sistēmām reāllaikā, draudu izlūkdatu sniedzējam būtu jāvāc izlūkdati vai informācija, kas aptver vismaz divas galvenās interešu jomas: mērķus, identificējot iespējamo uzbrukuma tvērumu visā finanšu vienībā, un draudus, identificējot attiecīgos apdraudējuma dalībniekus un iespējamos apdraudējuma scenārijus. Lai nodrošinātu, ka draudu izlūkdatu sniedzējs ņem vērā attiecīgos draudus finanšu vienībai, testētājiem, kontroles komandai un testu pārvaldniekiem būtu jāsniedz atsauksmes par draudu izlūkdatu ziņojuma projektu. Ja tā ir pieejama, draudu izlūkdatu sniedzējs kā pamatu valsts apdraudējuma ainai var izmantot vispārēju apdraudējuma ainu, ko attiecībā uz dalībvalsts finanšu nozari nodrošinājusi DVIT iestāde. Pamatojoties uz *TIBER-EU* sistēmas piemērošanu, draudu izlūkdatu vākšanas process parasti ilgst aptuveni četras nedēļas.

(19) Lai testētāji varētu gūt ieskatu, kā arī lai turpmāk pārskatītu darbības jomas specifikācijas dokumentu un mērķorientētu draudu izlūkdatu ziņojumu, kas nepieciešami sarkanās komandas testēšanas plāna pabeigšanai, ir būtiski, lai pirms DVIT sarkanās komandas testēšanas posma testētāji no draudu izlūkdatu sniedzēja saņemtu detalizētus paskaidrojumus par mērķorientētu draudu izlūkdatu ziņojumu un iespējamo apdraudējuma scenāriju analīzi.

(20) Lai testētāji varētu veikt reālistisku un visaptverošu testēšanu, kurā tiek izpildīti visi uzbrukuma posmi un sasniegtas atzīmes, sarkanās komandas aktīvās testēšanas posmam būtu jāatvēl pietiekams laiks. Pamatojoties uz pieredzi, kas gūta saistībā ar *TIBER-EU* sistēmu, atvēlētajam laikam vajadzētu būt vismaz 12 nedēļām, un tas būtu jānosaka, ņemot vērā iesaistīto pušu skaitu, DVIT darbības jomu, iesaistītās finanšu vienības vai vienību resursus, jebkādas ārējās prasības un finanšu vienības sniegtās pamatojošās informācijas pieejamību.

(21) Lai pienācīgi testētu finanšu vienības izstrādes sistēmas reāllaikā, sarkanās komandas aktīvās testēšanas posmā testētājiem būtu jāizmanto virkne taktiku, paņēmienu un procedūru (TPP). TPP attiecīgā gadījumā būtu jāietver izlūkošana (t. i., pēc iespējas lielāka apjoma informācijas apkopošana par mērķi), izmantošana par ieroci (t. i., informācijas analīze par infrastruktūru, iekārtām un darbiniekiem un sagatavošanās darbībām, kas raksturīgas mērķim), piegāde (t. i., aktīva pilnas darbības uzsākšana attiecībā uz mērķi), izmantošana (t. i., ja testētāju mērķis ir apdraudēt serverus, finanšu vienības tīklus un izmantot tās darbiniekus ar sociālās inženierijas starpniecību), kontrole un kustība (t. i., mēģinājumi pāriet no apdraudētajām sistēmām uz citām neaizsargātām vai augstvērtīgām sistēmām) un darbības attiecībā uz mērķi (t. i., turpmākas piekļuves panākšana apdraudētajām sistēmām un piekļuves iegūšana iepriekš saskaņotajai mērķa informācijai un datiem, par ko iepriekš panākta vienošanās sarkanās komandas testēšanas plānā).

(22) Veicot DVIT, testētājiem būtu jārīkojas, ņemot vērā uzbrukuma veikšanai pieejamo laiku, resursus un ētiskās un juridiskās robežas. Ja testētāji nespēj virzīties uz nākamo uzbrukuma plānoto posmu, kontroles komandai, vienojoties ar DVIT iestādi, būtu jāsniedz epizodiska palīdzība "atbalsta" veidā. Atbalstu var plaši iedalīt informatīvā atbalstā un piekļuves atbalstā, un tas var ietvert piekļuves nodrošināšanu IKT sistēmām vai iekšējiem tīkliem, lai turpinātu testu un koncentrētos uz nākamajiem uzbrukuma posmiem.

(23) Aktīvai sarkanās komandas izmantošanai testēšanas posmā, ja tas nepieciešams, lai izņēmuma apstākļos to pielietotu kā galējo līdzekli, kas ļauj turpināt DVIT, un pēc tam, kad ir izsmeltas visas alternatīvās iespējas, būtu jāizmanto uz sadarbību vērsta testēšanas darbība, kurā iesaistīti gan testētāji, gan zilā komanda. Veicot šādu ierobežotu purpursarkanās komandas izmantošanas darbību, var izmantot šādas metodes: "notvert un atbrīvot", kad testētāji mēģina turpināt scenārijus, tiek atklāti un pēc tam atsāk testēšanu, "kara spēles", kas ļauj īstenot sarežģītākus scenārijus, ar kuriem testē stratēģisku lēmumu pieņemšanu, vai "uz sadarbību vērsts koncepcijas pierādījums", kas testētājiem un zilās komandas locekļiem kontrolētā un uz sadarbību orientētā vidē ļauj kopīgi validēt konkrētus drošības pasākumus, rīkus vai paņēmienus.

(24) DVIT būtu jāizmanto kā mācīšanās pieredze, kas palīdz uzlabot finanšu vienību digitālās darbības noturību. Šajā sakarā zilajai komandai un testētājiem būtu jāatkārto uzbrukums un sadarbībā ar testētājiem jāpārskata pasākumi, kas veikti, lai mācītos no testēšanas pieredzes. Šajā nolūkā un lai nodrošinātu pienācīgu sagatavošanu, pirms jebkādu atkārtošanas darbību veikšanas visām atkārtošanas darbībās iesaistītajām pusēm būtu jādara pieejams sarkanās komandas testa ziņojums un zilās komandas testa ziņojums. Turklāt, lai maksimāli izmantotu mācīšanās pieredzi, slēgšanas posmā būtu jāveic purpursarkanās komandas izmantošanas darbība. Metodēm, kuras var pielietot purpursarkanās komandas izmantošanai slēgšanas posmā, būtu jāietver diskusijas par alternatīviem uzbrukuma scenārijiem, alternatīvu scenāriju izpēte par reāllaika sistēmām vai tādu plānoto scenāriju atkārtota izpēte par reāllaika sistēmām, kurus testētāji nav spējuši pabeigt vai izpildīt testēšanas posmā.

(25) Lai vēl vairāk atvieglotu visu DVIT iesaistīto pušu mācīšanās pieredzi, turpmāko testu vajadzībām un lai veicinātu finanšu vienību digitālās darbības noturību, attiecīgajām pusēm būtu savstarpēji jāsniedz atsauksmes par vispārējo procesu un jo īpaši jānosaka, kuras darbības ir sekmīgi virzījušās vai varētu tikt uzlabotas un kuri DVIT procesa aspekti ir labi darbojušies vai varētu tikt uzlaboti.

(26) Kompetentajām iestādēm, kas minētas Regulas (ES) 2022/2554 46. pantā, un DVIT iestādēm, ja tās ir dažādas iestādes, būtu jāsadarbojas, lai esošajos uzraudzības procesos iekļautu padziļinātu testēšanu, izmantojot DVIT. Šajā sakarā un lai apmainītos ar pareizu izpratni par DVIT konstatējumiem un to interpretāciju, ir lietderīgi, jo īpaši attiecībā uz testa kopsavilkuma ziņojumu un kļūdu novēršanas plāniem, izveidot ciešu sadarbību starp testu pārvaldniekiem, kuri bija iesaistīti DVIT, un atbildīgajiem uzraudzītājiem.

(27) Regulas (ES) 2022/2554 26. panta 8. punkta pirmajā daļā ir noteikts, ka finanšu vienībām ir pienākums katra trešā testa veikšanai noslēgt līgumus ar ārējiem testētājiem. Ja finanšu vienības testētāju grupā iekļauj gan iekšējos, gan ārējos testētājus, minētā panta nolūkos to vajadzētu uzskatīt par DVIT, ko veic ar iekšējiem testētājiem.

(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"), vienojoties ar Eiropas Centrālo banku.

(29) Eiropas uzraudzības iestādes veica atklātu sabiedrisko apspriešanu par regulatīvo tehnisko standartu projektu, kas ir šīs regulas pamatā, izvērtēja potenciālās saistītās izmaksas un ieguvumus un lūdza atzinumu no Banku nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 ([3]) 37. pantu, no Apdrošināšanas un pārapdrošināšanas nozares ieinteresēto personu grupas un Aroda pensiju nozares ieinteresēto personu grupas, kas izveidotas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1094/2010 ([4]) 37. pantu, un no Vērtspapīru un tirgu nozares ieinteresēto personu grupas, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1095/2010 ([5]) 37. pantu.

(30) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([6]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas sniedza atzinumu 2024. gada 20. augustā,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "kontroles komanda" ir komanda, kuras sastāvā ir tās finanšu vienības darbinieki, kurai veic testēšanu, un, attiecīgā gadījumā ņemot vērā DVIT darbības jomu, trešo personu, kas sniedz pakalpojumus, un jebkuras citas personas darbinieki, kuri pārvalda testu;

2) "kontroles komandas vadītājs" ir finanšu vienības darbinieks, kas ir atbildīgs par visu finanšu vienības ar DVIT saistīto darbību veikšanu konkrētā testa kontekstā;

3) "zilā komanda" ir tie finanšu vienības darbinieki un attiecīgā gadījumā trešo personu, kas sniedz pakalpojumus finanšu vienībai, darbinieki, kā arī jebkura cita puse, ko uzskata par būtisku, ņemot vērā DVIT darbības jomu, kuri, uzturot savus drošības parametrus pret simulētiem vai reāliem uzbrukumiem, aizsargā finanšu vienības tīklu un informācijas sistēmu izmantošanu un kuri nav informēti par DVIT;

4) "zilās komandas uzdevumi" ir uzdevumi, ko parasti veic zilā komanda, piemēram, drošības operāciju centrs (DOC), IKT infrastruktūras pakalpojumi, palīdzības dienesta pakalpojumi, incidentu pārvaldības pakalpojumi darbības līmenī;

5) "sarkanā komanda" ir iekšējie vai ārējie testētāji, ar kuriem noslēgts līgums vai kuri norīkoti veikt DVIT;

6) "purpursarkanās komandas izmantošana" ir uz sadarbību vērsta testēšanas darbība, kurā piedalās gan testētāji, gan zilā komanda;

([3]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

7) “DVIT iestāde” ir jebkura no turpmāk minētajām:

a) vienota publiskā iestāde finanšu nozarē, kas izraudzīta saskaņā ar Regulas (ES) 2022/2554 26. panta 9. punktu;

b) iestāde finanšu nozarē, kurai saskaņā ar Regulas (ES) 2022/2554 26. panta 10. punktu ir deleģēta dažu vai visu ar DVIT saistīto uzdevumu izpilde;

c) jebkura no Regulas (ES) 2022/2554 46. pantā minētajām kompetentajām iestādēm;

8) “DVIT kiberkomanda” ir DVIT iestāžu darbinieki, kuri atbild par jautājumiem, kas saistīti ar DVIT;

9) “testu pārvaldnieki” ir darbinieki, kas izraudzīti vadīt DVIT iestādes darbības attiecībā uz konkrētu DVIT, lai uzraudzītu atbilstību šai regulai;

10) “draudu izlūkdatu sniedzējs” ir eksperti, ar kuriem finanšu vienība ir noslēgusi līgumus par katru DVIT un kuri nav saistīti ar finanšu vienību un vienai grupai piederošiem IKT pakalpojumu sniedzējiem, ja tādi ir, un kuri apkopo un analizē mērķorientētus draudu izlūkdatus, kas attiecas uz finanšu vienībām konkrētas DVIT darbības ietvaros, un izstrādā atbilstīgus un reālistiskus apdraudējuma scenārijus;

11) “DVIT pakalpojumu sniedzēji” ir testētāji un draudu izlūkdatu sniedzēji;

12) “atbalsts” ir palīdzība vai informācija, ko kontroles komanda sniedz testētājiem, lai testētāji varētu turpināt īstenot uzbrukuma ceļu, ja viņi paši nespēj virzīties uz priekšu un ja nav citas pieņemamas alternatīvas, tostarp attiecībā uz nepietiekamu laiku vai resursiem konkrētā DVIT;

13) “uzbrukuma ceļš” ir maršruts, ko testētāji veic DVIT sarkanās komandas aktīvās testēšanas posmā, lai sasniegtu minētajai DVIT norādītās atzīmes;

14) “atzīmes” ir IKT sistēmu, ar kurām atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas, galvenie mērķi, kurus testētāji cenšas sasniegt testa gaitā;

15) “sensitīva informācija” ir informācija, ko var viegli izmantot, lai veiktu uzbrukumus finanšu vienības IKT sistēmām, intelektuālais īpašums, konfidenciāli darījumdarbības dati vai personas dati, kas var tieši vai netieši kaitēt finanšu vienībai un tās ekosistēmai, ja tā nonāktu ļaunprātīgu personu rokās;

16) “kopums” ir visas finanšu vienības, kas piedalās apvienotā DVIT saskaņā ar Regulas (ES) 2022/2554 26. panta 4. punktu;

17) “uzņēmēja dalībvalsts” ir uzņēmēja dalībvalsts saskaņā ar Savienības nozaru tiesību aktiem, kas piemērojami katrai finanšu vienībai;

18) “kopīga DVIT” ir DVIT, kas nav Regulas (ES) 2022/2554 26. panta 4. punktā minētā apvienotā DVIT un kurā iesaistītas vairākas finanšu vienības, kas izmanto vienu un to pašu IKT pakalpojumu sniedzēju, kurš pieder vienai grupai, vai kuras pieder pie vienas un tās pašas grupas un kopīgi izmanto IKT sistēmas.

2. pants

To finanšu vienību identificēšana, kurām ir pienākums veikt DVIT

1. To, vai finanšu vienībai ir pienākums veikt DVIT, ņemot vērā attiecīgās finanšu vienības ietekmi, tās sistēmisko raksturu un IKT riska profilu, DVIT iestādes novērtē, pamatojoties uz visiem šādiem kritērijiem:

a) ar ietekmi saistīti un ar sistēmisku raksturu saistīti faktori:

i) finanšu vienības lielums, ko nosaka, pamatojoties uz to, vai finanšu vienība sniedz finanšu pakalpojumus vienā vai vairākās dalībvalstīs, un salīdzinot finanšu vienības darbības ar citu finanšu vienību, kas sniedz līdzīgus pakalpojumus, darbībām;

ii) apmērs un veids, kādā finanšu vienība ir savstarpēji saistīta ar citām finanšu vienībām finanšu nozarē vienā vai vairākās dalībvalstīs;

iii) finanšu vienības sniegto pakalpojumu kritiskums vai svarīgums finanšu nozarei;

iv) finanšu vienības sniegto pakalpojumu aizstājamība;

v) finanšu vienības darījumdarbības modeļa un saistīto pakalpojumu un procesu sarežģītība;

vi) vai finanšu vienība ir daļa no sistēmiska rakstura grupas Savienības vai valsts līmenī finanšu nozarē un kopīgi izmanto IKT sistēmas;

b) ar IKT risku saistīti faktori:

i) finanšu vienības riska profils;

ii) finanšu vienības apdraudējuma aina;

iii) cik lielā mērā finanšu vienības kritiski svarīgās vai svarīgās funkcijas vai to atbalsta funkcijas ir atkarīgas no IKT sistēmām un procesiem;

iv) finanšu vienības IKT arhitektūras sarežģītība;

v) IKT pakalpojumi un funkcijas, ko atbalsta trešās personas, kas sniedz IKT pakalpojumus, un līgumisko vienošanos ar trešām personām, kas sniedz IKT pakalpojumus, vai ar IKT pakalpojumu sniedzējiem, kuri pieder vienai grupai, skaits un veids;

vi) visu to uzraudzības pārbaužu rezultāti, kas ir būtiski finanšu vienības IKT gatavības līmeņa novērtēšanai;

vii) IKT darbības nepārtrauktības plānu un IKT reaģēšanas un seku novēršanas plānu gatavības līmenis;

viii) operacionālo IKT drošības pasākumu attiecībā uz atklāšanu un mazināšanu gatavības līmenis, tostarp spēja:

1) pastāvīgi uzraudzīt finanšu vienības IKT infrastruktūru;

2) atklāt ar IKT saistītus incidentus reāllaikā;

3) analizēt 2. punktā minētos incidentus;

4) laikus un rezultatīvi reaģēt uz 2. punktā minētajiem incidentiem;

ix) vai finanšu vienība ir daļa no grupas, kas darbojas finanšu nozarē Savienības vai valsts līmenī un kam ir kopīgas IKT sistēmas.

Piemērojot a) apakšpunkta i) punktu, DVIT iestāde, ja iespējams, apsver:

a) finanšu vienības tirgus daļas pozīciju Savienības un valsts līmenī;

b) finanšu vienības piedāvāto darbību klāstu;

c) finanšu vienības sniegto pakalpojumu vai Savienības un valsts līmenī veikto darbību tirgus daļu.

Piemērojot a) apakšpunkta v) punktu, DVIT iestāde, ja iespējams, apsver:

a) vai finanšu vienība izmanto vairāk nekā vienu darījumdarbības modeli;

b) dažādu darījumdarbības procesu un saistīto pakalpojumu savstarpējo savienojamību.

2. Ja vien 1. punktā minētais novērtējums attiecībā uz finanšu vienību nenorāda, ka tās ietekme, ar minēto finanšu vienību saistītās bažas par finanšu stabilitāti vai tās IKT riska profils nepamato DVIT veikšanu, DVIT iestādes pieprasa veikt DVIT visām turpmāk minētajām finanšu vienībām:

a) kredītiestādēm, kas atbilst kādam no šādiem nosacījumiem:

i) tās ir identificētas kā globālas sistēmiski nozīmīgas iestādes (G-SNI) saskaņā ar Eiropas Parlamenta un Padomes Direktīvas 2013/36/ES ([7]) 131. pantu;

ii) tās ir identificētas kā citas sistēmiski nozīmīgas iestādes (C-SNI) saskaņā ar Direktīvas 2013/36/ES 131. pantu;

iii) tās ir daļa no G-SNI vai C-SNI;

([7]) Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp., ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) maksājumu iestādēm, kas katrā no diviem kalendārajiem gadiem pirms DVIT iestādes veiktā novērtējuma ir pārsniegušas 150 miljardus EUR no maksājumu darījumu kopējās vērtības, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/2366 ([8]) 4. panta 5. punktā;

c) elektroniskās naudas iestādēm, kas katrā no diviem kalendārajiem gadiem pirms DVIT iestādes veiktā novērtējuma ir pārsniegušas 150 miljardus EUR no maksājumu darījumu kopējās vērtības, kā noteikts Direktīvas (ES) 2015/2366 4. panta 5. punktā, vai 40 miljardus EUR no apgrozībā esošas elektroniskās naudas kopējās vērtības;

d) centrālajiem vērtspapīru depozitārijiem;

e) centrālajiem darījumu partneriem;

f) tādām tirdzniecības vietām ar elektronisku tirdzniecības sistēmu, kas atbilst kādam no šādiem kritērijiem:

i) tirdzniecības vietai katrā no diviem kalendārajiem gadiem pirms DVIT iestādes veiktā novērtējuma apgrozījuma ziņā valsts līmenī ir lielākā tirgus daļa kādā no turpmāk minētajām kategorijām:

1) pārvedami vērtspapīri, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES ([9]) 4. panta 1) punkta 44) apakšpunkta a) punktā;

2) pārvedami vērtspapīri, kā definēts Direktīvas 2014/65/ES 4. panta 1) punkta 44) apakšpunkta b) punktā;

3) atvasinātie instrumenti, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 600/2014 ([10]) 2. panta 1. punkta 29) apakšpunktā;

4) strukturētā finansējuma produkti, kā definēts Regulas (ES) Nr. 600/2014 2. panta 1. punkta 28) apakšpunktā;

5) emisijas kvotas, kā definēts Direktīvas 2014/65/ES I pielikuma C iedaļas 11. punktā;

ii) tirdzniecības vietas tirgus daļa apgrozījuma ziņā Savienības līmenī pārsniedz 5 % katrā no diviem kalendārajiem gadiem pirms DVIT iestādes veiktā novērtējuma kādā no turpmāk minētajiem:

1) uzņēmumu akcijas un citi vērtspapīri, kas ir līdzvērtīgi uzņēmumu, personālsabiedrību vai citu vienību akcijām, un depozitārie sertifikāti attiecībā uz akcijām;

2) obligācijas vai cita veida parāda vērtspapīri, tostarp depozitārie sertifikāti attiecībā uz šādiem vērtspapīriem;

3) atvasinātie instrumenti, kā definēts Regulas (ES) Nr. 600/2014 2. panta 1. punkta 29) apakšpunktā;

4) strukturētā finansējuma produkti, kā definēts Regulas (ES) Nr. 600/2014 2. panta 1. punkta 28) apakšpunktā;

5) emisijas kvotas, kā definēts Direktīvas 2014/65/ES I pielikuma C iedaļas 11. punktā;

([8]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp., ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Eiropas Parlamenta un Padomes Direktīva 2014/65/ES (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/EK un Direktīvu 2011/61/ES (OV L 173, 12.6.2014., 349. lpp., ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) 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).

g) apdrošināšanas un pārapdrošināšanas sabiedrībām, kas atbilst visiem šādiem kritērijiem:

i) to bruto parakstītā prēmija (*GWP*) pārsniedz 1 500 000 000 EUR;

ii) to tehniskās rezerves pārsniedz 10 000 000 000 EUR;

iii) apdrošināšanas sabiedrības, kuras veic tikai dzīvības apdrošināšanas darbības vai kuras veic gan dzīvības, gan nedzīvības apdrošināšanas darbības un kuru kopējie aktīvi pārsniedz 3,5 % no dalībvalstī iedibināto apdrošināšanas un pārapdrošināšanas sabiedrību kopējo aktīvu summas, kas novērtēti saskaņā ar Eiropas Parlamenta un Padomes Direktīvas 2009/138/EK ([11]) 75. pantu.

Šā punkta f) apakšpunkta ii) punkta nolūkos, ja tirdzniecības vieta ir daļa no grupas, kurai ir kopīgas IKT sistēmas, vai tas pats IKT pakalpojumu sniedzējs, kurš pieder vienai grupai, ņem vērā vērtspapīru un atvasināto instrumentu līgumu apgrozījumu par vienu un to pašu grupu visās tirdzniecības vietās, kuras iedibinātas Savienībā.

Šā panta g) apakšpunkta nolūkos DVIT iestādes identificē visu apdrošināšanas un pārapdrošināšanas sabiedrību apakškopu, piemērojot g) apakšpunkta i), ii) un iii) punktā noteiktos kritērijus. Apdrošināšanas un pārapdrošināšanas sabiedrībām, kas iekļautas minētajā apakškopā, ir pienākums veikt DVIT, ja tās atbilst arī kādam no šādiem kritērijiem:

a) bruto parakstītā prēmija (*GWP*) pārsniedz 3 000 000 000 EUR;

b) tehniskās rezerves pārsniedz 30 000 000 000 EUR;

c) kopējie aktīvi pārsniedz 10 % no apdrošināšanas un pārapdrošināšanas sabiedrību, kuras iedibinātas dalībvalstī, saskaņā ar Direktīvas 2009/138/EK 75. pantu novērtēto kopējo aktīvu summas.

3. Ja vairāk nekā viena finanšu vienība, kas pieder pie vienas un tās pašas grupas un kurai ir kopīgas IKT sistēmas, vai ja vairāk nekā viena finanšu vienība, kas izmanto vienu un to pašu IKT pakalpojumu sniedzēju, kurš pieder vienai grupai, atbilst 2. punktā izklāstītajiem kritērijiem, minēto finanšu vienību DVIT iestādes saskaņā ar 16. panta 2. punktu pieņem lēmumu par to, vai pienākums atsevišķi veikt DVIT ir būtisks minētajām finanšu vienībām.

Ja pirmajā daļā minētās finanšu vienību grupas mātesuzņēmuma DVIT iestāde atšķiras no grupas finanšu vienību DVIT iestādēm, pie minētās grupas piederošo finanšu vienību DVIT iestādes apspriežas ar minēto iestādi par to, vai ir lietderīgi DVIT veikt atsevišķi.

3. pants

DVIT kiberkomanda un DVIT testu pārvaldnieki

1. DVIT iestāde atbildību par to darbību koordinēšanu, kas saistītas ar DVIT, uztic DVIT kiberkomandai. DVIT kiberkomanda sastāv no testu pārvaldniekiem, kas norīkoti, lai pārraudzītu atsevišķu DVIT.

2. DVIT iestāde katram testam izraugās testa pārvaldnieku un vismaz vienu aizvietotāju.

3. Testu pārvaldnieki uzrauga, vai tiek ievērotas šajā regulā noteiktās prasības, un nodrošina, ka tās tiek ievērotas.

([11]) Eiropas Parlamenta un Padomes Direktīva 2009/138/EK (2009. gada 25. novembris) par uzņēmējdarbības uzsākšanu un veikšanu apdrošināšanas un pārapdrošināšanas jomā (Maksātspēja II) (OV L 335, 17.12.2009., 1. lpp., ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Testa pārvaldnieks paziņo finanšu vienībai DVIT kiberkomandas kontaktinformāciju, izmantojot 9. panta 1. punktā minēto paziņojumu.

5. DVIT iestāde piedalās visos DVIT posmos.

4. pants

Organizatoriskie pasākumi finanšu vienībām

1. Finanšu vienības ieceļ kontroles komandas vadītāju, kas ir atbildīgs par DVIT ikdienas pārvaldību un kontroles komandas lēmumiem un darbībām.

2. Finanšu vienības nosaka organizatoriskus un procesuālus pasākumus, ar kuriem nodrošina, ka:

a) pamatojoties uz vajadzību pēc informācijas, piekļuve informācijai par jebkuru plānotu vai notiekošu DVIT tiek nodrošināta tikai kontroles komandai, vadības struktūrai, testētājiem, draudu izlūkdatu sniedzējam un DVIT iestādei;

b) kontroles komanda apspriežas ar testu pārvaldniekiem pirms jebkura zilās komandas dalībnieka iesaistīšanas DVIT;

c) kontroles komanda ir informēta par visiem gadījumiem, kad finanšu vienības darbinieki vai trešās personas, kas sniedz pakalpojumus, ir konstatējuši, ka notiek DVIT; ja no tiem izrietošā reaģēšana uz incidentiem eskalējas, vajadzības gadījumā kontroles komanda šādu eskalāciju mazina;

d) ir izstrādāti tādi pasākumi attiecībā uz DVIT slepenību, ko ievēro finanšu vienības darbinieki, attiecīgo trešo personu, kas sniedz IKT pakalpojumus, darbinieki, testētāji un draudu izlūkdatu sniedzēji;

e) kontroles komanda pēc pieprasījuma sniedz testu pārvaldniekiem visu informāciju, kas attiecas uz DVIT;

f) ja iespējams, DVIT iesaistītās puses uz testēšanu atsaucas, tikai izmantojot kodētus nosaukumus.

5. pants

DVIT riska pārvaldība

1. Šīs regulas 9. pantā minētajā sagatavošanas posmā kontroles komanda novērtē riskus, kas saistīti ar finanšu vienības kritiski svarīgu vai svarīgu funkciju izstrādes sistēmu testēšanu reāllaikā, tostarp iespējamo ietekmi uz:

a) finanšu nozari;

b) finanšu stabilitāti Savienības vai valsts līmenī.

Kontroles komanda minēto ietekmi pārskata visā testēšanas gaitā.

2. Riska novērtēšanas un pārvaldības nolūkos kontroles komanda ņem vērā vismaz šādus risku veidus, kas saistīti ar:

a) piekļuves piešķiršanu draudu izlūkdatu sniedzējam un ārējiem testētājiem attiecīgā gadījumā sensitīvai informācijai par finanšu vienību;

b) DVIT neatbilstību Regulai (ES) 2022/2554 un šai regulai, ja šādas neatbilstības dēļ trūkst Regulas (ES) 2022/2554 26. panta 7. punktā minētā apliecinājuma, tostarp, ja šāda neatbilstība ir saistīta ar DVIT konfidencialitātes pārkāpumiem vai ētiskas rīcības trūkumu;

c) krīzes un incidentu eskalāciju;

d) sarkanās komandas aktīvo posmu, tostarp riskiem, kas saistīti ar kritiski svarīgu darbību pārtraukšanu un datu bojājumu testētāju darbību dēļ, un tā iespējamo ietekmi uz trešām personām;

e) zilās komandas darbību, tostarp riskiem, kas saistīti ar kritiski svarīgu darbību pārtraukšanu un datu bojājumu zilās komandas darbību dēļ, un tās iespējamo ietekmi uz trešām personām;

f) to sistēmu nepilnīgu atjaunošanu, kuras ir skārusi DVIT.

6. pants

Apvienotu vai kopīgu DVIT riska pārvaldība

1. Kopīgas DVIT vai apvienotas DVIT gadījumā katras finanšu vienības kontroles komanda veic savu riska novērtējumu un nosaka savus riska pārvaldības pasākumus.

2. Šīs regulas 16. panta 3. punkta b) apakšpunktā minētās izraudzītās finanšu vienības kontroles komanda vai saskaņā ar Regulas (ES) 2022/2554 26. panta 4. punktu izraudzītā finanšu vienība novērtē riskus, kas saistīti ar vairāku finanšu vienību iesaistīšanos DVIT. Iesaistīto finanšu vienību kontroles komandas sadarbojas ar izraudzītās finanšu vienības kontroles komandu, lai identificētu iespējamos kopīgos riskus.

7. pants

DVIT pakalpojumu sniedzēju atlase

1. Kontroles komanda veic pasākumus nolūkā pārvaldīt ar DVIT saistītos riskus, un jo īpaši nodrošina, ka attiecībā uz katru DVIT:

a) draudu izlūkdatu sniedzējs un ārējie testētāji iesniedz kontroles komandai detalizētu *curriculum vitae* un sertifikātu kopijas, kas saskaņā ar atzītiem tirgus standartiem ir piemēroti to darbību veikšanai;

b) draudu izlūkdatu sniedzējs un ārējais testētājs ir pienācīgi un pilnībā apdrošināts ar atbilstošu profesionālās darbības apdrošināšanu, tostarp pret ļaunprātīgas rīcības un nolaidības riskiem;

c) draudu izlūkdatu sniedzējs nodrošina vismaz trīs atsauksmes no iepriekšējiem norīkojumiem ielaušanās testēšanas un sarkanās komandas testēšanas kontekstā;

d) ārējie testētāji nodrošina vismaz piecas atsauksmes no iepriekšējiem norīkojumiem saistībā ar ielaušanās testēšanu un sarkanās komandas testēšanu;

e) draudu izlūkdatu sniedzēja darbinieki, kas norīkoti veikt DVIT:

i) to sastāvā ir pārvaldnieks ar vismaz piecu gadu pieredzi draudu izlūkdatu jomā un vismaz viens papildu loceklis ar vismaz divu gadu pieredzi draudu izlūkdatu jomā;

ii) ir ar plašām un atbilstoša līmeņa profesionālajām zināšanām un prasmēm, tostarp tie:

1) pārzina izlūkdatu vākšanas taktikas, paņēmienus un procedūras;

2) ir ar ģeopolitiskām un tehniskām zināšanām un zināšanām par nozari;

3) ar atbilstošām komunikācijas prasmēm skaidri izklāstīt iesaistes rezultātus un ziņot par tiem;

iii) ir kopīgi piedalījušies vismaz trijos iepriekšējos norīkojumos draudu izlūkdatu jomā ielaušanās testēšanas un sarkanās komandas testēšanas kontekstā;

iv) vienlaikus neveic zilās komandas uzdevumus vai citus pakalpojumus, kas var radīt interešu konfliktu attiecībā uz tādā DVIT iesaistīto finanšu vienību, trešo personu, kas sniedz IKT pakalpojumus, vai vienai grupai piederošu IKT pakalpojumu sniedzēju, kurai tie ir norīkoti;

v) ir nošķirti no viena un tā paša DVIT pakalpojumu sniedzēja darbiniekiem, kas nodrošina ārējos testētājus vienai un tai pašai DVIT, un tiem neatskaitās;

f) attiecībā uz ārējiem testētājiem – DIVIT veikšanai norīkotā sarkanā komanda:

i) sastāv vismaz no pārvaldnieka ar vismaz piecu gadu pieredzi ielaušanās testēšanā un sarkanās komandas testēšanā, kā arī vismaz no diviem papildu testētāji, no kuriem katrs vismaz divus gadus ir veicis ielaušanās testēšanu un sarkanās komandas testēšanu;

ii) ir ar plašām un atbilstoša līmeņa profesionālajām zināšanām un prasmēm, tostarp zināšanām par finanšu vienības darījumdarbību, izlūkošanu, riska pārvaldību, mūķu izstrādi, fizisku ielaušanos, sociālo inženieriju, ievainojamības analīzi, kā arī atbilstīgām komunikācijas prasmēm skaidri izklāstīt iesaistes rezultātus un ziņot par tiem;

iii) ir kopīgi piedalījusies vismaz piecos iepriekšējos norīkojumos saistībā ar ielaušanās testēšanu un sarkanās komandas testēšanu;

iv) nav nodarbināta un nesniedz pakalpojumus draudu izlūkdatu sniedzējam, kas vienlaikus veic zilās komandas uzdevumus vai nu DVIT iesaistītai finanšu vienībai, trešai personai, kas sniedz IKT pakalpojumus, vai IKT pakalpojumu sniedzējam, kurš pieder vienai grupai;

v) ir nošķirta no visiem tā paša DVIT pakalpojumu sniedzēja, kas vienlaikus sniedz draudu izlūkdatu pakalpojumus vienai un tai pašai DVIT, darbiniekiem;

g) testēšanas beigās testētāji un draudu izlūkdatu sniedzējs veic atjaunošanas procedūras, tostarp nodrošina informācijas dzēšanu saistībā ar parolēm, akreditācijas datiem un citām slepenām atslēgām, kas apdraudētas DVIT laikā, nodrošina saziņu ar finanšu vienībām par apdraudētajiem kontiem, nodrošina citu testēšanas laikā savākto datu drošu apkopošanu, glabāšanu, pārvaldību un iznīcināšanu;

h) papildus g) apakšpunktā minētajām atjaunošanas procedūrām testēšanas beigās testētāji veic šādas atjaunošanas procedūras:

i) vadības un kontroles deaktivēšana;

ii) darbības jomas un datuma automātiska deaktivēšana;

iii) lūku un citas ļaunprogrammatūras likvidēšana;

iv) paziņojums par iespējamiem pārkāpumiem;

v) procedūras turpmākai dublējumu atjaunošanai, kas var attiekties uz testa laikā instalētu ļaunprogrammatūru vai rīkiem;

vi) zilās komandas darbību uzraudzība un kontroles komandas informēšana par jebkādiem iespējamiem atklājumiem;

i) testētāji un draudu izlūkdatu sniedzējs neveic un nepiedalās nevienā no šādām darbībām:

i) finanšu vienības un tās trešo personu, kas sniedz IKT pakalpojumus, aprīkojuma neatļauta iznīcināšana, ja tāda ir;

ii) finanšu vienības un tās trešo personu, kas sniedz IKT pakalpojumus, informācijas un IKT aktīvu nekontrolēta pārveidošana, ja tāda ir;

iii) finanšu vienības kritiski svarīgu vai svarīgu funkciju nepārtrauktības tīša apdraudēšana;

iv) ārpus darbības jomas esošu sistēmu neatļauta izmantošana;

v) testa rezultātu neatļauta izpaušana.

2. Lai pierādītu atbilstību 1. punkta a) līdz f) apakšpunktam, kontroles komanda reģistrē testētāju un draudu izlūkdatu sniedzēju iesniegto dokumentāciju.

Izņēmuma apstākļos finanšu vienības var slēgt līgumus ar ārējiem testētājiem un draudu izlūkdatu sniedzējiem, kas neatbilst vienai vai vairākām 1. punkta a)–f) apakšpunktā izklāstītajām prasībām, ar noteikumu, ka minētās finanšu vienības pieņem pasākumus, kas ir piemēroti tādu risku mazināšanai, kas saistīti ar neatbilstību minētajiem punktiem, un reģistrē minētos pasākumus.

8. pants

Apvienotas vai kopīgas DVIT specifika

1. Ja vien vadošā DVIT iestāde nav nolēmusi citādi, gadījumā, kad apvienotā vai kopīgā DVIT ir iesaistītas vairākas finanšu vienības, kas identificētas saskaņā ar 16. panta 2. vai 4. punktu, katra finanšu vienība ievēro ikvienu no 9.–15. pantā izklāstītajiem posmiem.

2. Ja vien šajā regulā nav noteikts citādi, gadījumā, kad vairākas DVIT iestādes ir iesaistītas kopīgā DVIT vai apvienotā DVIT, kā minēts 16. panta 3. vai 5. punktā, atsauces 9.–15. pantā uz "DVIT iestādi" saprot kā atsauci uz vadošo DVIT iestādi šādai apvienotai vai kopīgai DVIT.

9. pants

Sagatavošanas posms

1. Finanšu vienība, kas identificēta saskaņā ar Regulas (ES) 2022/2554 26. panta 8. punkta trešo daļu, uzsāk DVIT pēc DVIT iestādes paziņojuma par to, ka DVIT ir jāveic.

2. Finanšu vienība trīs mēnešu laikā pēc 1. punktā minētā paziņojuma saņemšanas iesniedz testu pārvaldniekiem visu turpmāk minēto informāciju par DVIT uzsākšanu:

a) projekta nolikumu, tostarp augsta līmeņa projekta plānu, kurā ietverta I pielikumā izklāstītā informācija;

b) kontroles komandas vadītāja kontaktinformāciju;

c) attiecīgā gadījumā informāciju par iekšējo vai ārējo testētāju, vai abu paredzēto izmantošanu, kā sīki izklāstīts 15. pantā;

d) informāciju par saziņas kanāliem, kas izmantojami DVIT laikā;

e) DVIT kodētu nosaukumu.

3. Ja 2. punkta a)–e) apakšpunktā minētā informācija ir pilnīga un nodrošina DVIT piemērotību un rezultatīvu darbību, DVIT iestāde apstiprina finanšu vienības sniegto informāciju par DVIT uzsākšanu un par to paziņo finanšu vienībai.

4. Pēc tam, kad DVIT iestāde ir apstiprinājusi informāciju par DVIT uzsākšanu, finanšu vienība izveido kontroles komandu, lai atbalstītu kontroles komandas vadītāju, kurš veic šādus uzdevumus:

a) precizē saziņas kanālus un procesus kontroles komandā, ar testētājiem un draudu izlūkdatu sniedzējiem visos jautājumos, kas saistīti ar DVIT;

b) informē finanšu vienības vadības struktūru par DVIT progresu un saistītajiem riskiem;

c) pieņem lēmumus DVIT gaitā, pamatojoties uz speciālajām zināšanām attiecīgajā jomā;

d) veic DVIT izpildi saskaņā ar šo regulu;

e) atlasa draudu izlūkdatu sniedzēju DVIT vajadzībām;

f) atlasa ārējos testētājus, iekšējos testētājus vai abus;

g) sagatavo darbības jomas specifikācijas dokumentu.

5. Ja DVIT iestāde uzskata, ka kontroles komandas sākotnējais sastāvs un visas turpmākās izmaiņas tajā ir piemērotas 4. punktā minēto uzdevumu veikšanai, DVIT iestāde apstiprina kontroles komandu un par to paziņo kontroles komandas vadītājam.

6. Finanšu vienība sešu mēnešu laikā pēc paziņojuma saņemšanas no 1. punktā minētās DVIT iestādes iesniedz testu pārvaldniekiem darbības jomas specifikācijas dokumentu, kurā ietverta visa II pielikumā izklāstītā informācija. Finanšu vienības vadības struktūra apstiprina darbības jomas specifikācijas dokumentu.

7. Attiecībā uz kritiski svarīgu vai svarīgu funkciju iekļaušanu DVIT darbības jomā finanšu vienības ņem vērā šādus kritērijus:

a) funkcijas kritiskums vai svarīgums un tās iespējamā ietekme uz finanšu nozari un finanšu stabilitāti Savienības un valsts līmenī;

b) funkcijas svarīgums finanšu vienības ikdienas darījumdarbībā;

c) funkcijas aizstājamība;

d) savstarpējā savienojamība ar citām funkcijām;

e) funkcijas ģeogrāfiskā atrašanās vieta;

f) citu vienību atkarība no funkcijas nozarē;

g) draudu izlūkdati par funkciju, ja tādi ir pieejami.

8. Kontroles komanda informāciju par DVIT uzsākšanu un darbības jomas specifikācijas dokumentu testētājiem un draudu izlūkdatu sniedzējiem nodod pēc līgumu noslēgšanas. Kontroles komanda testētājus un draudu izlūkdatu sniedzējus informē par testēšanas procesu, kas jāievēro.

9. Finanšu vienība nodrošina, ka testētāju un draudu izlūkdatu sniedzēju iepirkums vai norīkošana tiek pabeigta pirms testēšanas posma uzsākšanas.

10. Pirms testēšanas posma uzsākšanas kontroles komanda apspriežas ar testu pārvaldniekiem par DVIT riska novērtējumu un riska pārvaldības pasākumiem. Kontroles komanda pārskata riska novērtējumu vai riska pārvaldības pasākumus, ja DVIT iestāde uzskata, ka tie pienācīgi nenovērš DVIT riskus.

11. Kontroles komanda novērtē, vai draudu izlūkdatu sniedzēji un testētāji, kurus tie apsver iesaistīt DVIT, atbilst prasībām, kas noteiktas Regulas (ES) 2022/2554 27. pantā un šīs regulas 7. panta 1. punktā, un dokumentē minētā novērtējuma rezultātus. Kontroles komanda atlasa draudu izlūkdatu sniedzējus saskaņā ar minēto novērtējumu un savu riska pārvaldības praksi. Pirms līguma noslēgšanas ar atlasītajiem draudu izklūkdatu sniedzējiem un ārējiem testētājiem kontroles komanda sniedz testu pārvaldniekiem pierādījumus par minēto draudu izlūkdatu sniedzēju un testētāju atbilstību Regulas (ES) 2022/2554 27. pantā un šīs regulas 7. panta 1. punktā noteiktajām prasībām. Kontroles komanda neslēdz līgumus ar atlasītajiem draudu izklūkdatu sniedzējiem un ārējiem testētājiem, ja DVIT iestāde uzskata, ka atlasītie draudu izlūkdatu sniedzēji un ārējie testētāji neatbilst Regulas (ES) 2022/2554 27. pantā noteiktajām prasībām vai šīs regulas 7. panta 1. punktā noteiktajām prasībām, vai papildu prasībām, kas izriet no valsts drošības tiesību aktiem saskaņā ar Savienības tiesību aktiem, vai ja finanšu vienība neatbilst šīs regulas 7. panta 2. punkta pirmajai daļai, vai ja nav izpildīti šīs regulas 7. panta 2. punkta otrajā daļā minētie apstākļi.

12. Ja darbības jomas specifikācijas dokuments ir pilnīgs un nodrošina piemērotas un rezultatīvas DVIT veikšanu, DVIT iestāde apstiprina minēto dokumentu un par to informē kontroles komandas vadītāju.

10. pants

Testēšanas posms: draudu izlūkdati

1. Pēc tam, kad DVIT iestāde ir apstiprinājusi darbības jomas specifikācijas dokumentu, draudu izlūkdatu sniedzējs analizē vispārējus un nozarei specifiskus draudu izlūkdatus, kas attiecas uz finanšu vienību. Ja DVIT iestāde ir nodrošinājusi informāciju par vispārēju apdraudējuma ainu dalībvalsts finanšu nozarei, draudu izlūkdatu sniedzējs var izmantot šo ainu kā pamatu valsts apdraudējuma ainai. Draudu izlūkdatu sniedzējs identificē kiberdraudus un esošo vai iespējamo ievainojamību attiecībā uz finanšu vienību. Turklāt draudu izlūkdatu sniedzējs vāc informāciju un analizē konkrētus, īstenojamus un kontekstualizētus mērķa un draudu izlūkdatus par finanšu vienību, tostarp apspriežoties ar kontroles komandu un testu pārvaldniekiem.

2. Draudu izlūkdatu sniedzējs izklāsta attiecīgos draudus un mērķorientētos draudu izlūkdatus un ierosina vajadzīgos scenārijus kontroles komandai, testētājiem un testu pārvaldniekiem. Ierosinātie scenāriji atšķiras atkarībā no identificētajiem apdraudējuma dalībniekiem un ar tiem saistītajām taktikām, paņēmieniem un procedūrām, un tie ir vērsti uz katru kritiski svarīgu vai svarīgu funkciju DVIT darbības jomā.

3. Lai veiktu DVIT, kontroles komandas vadītājs atlasa vismaz trīs scenārijus, pamatojoties uz visiem šādiem elementiem:

a) draudu izlūkdatu sniedzēja ieteikums un katra scenārija draudu vadītais raksturs;

b) testu pārvaldnieku sniegtais ieguldījums;

c) ierosināto izpildes scenāriju īstenojamība, pamatojoties uz testētāju eksperta līmeņa slēdzienu;

d) finanšu vienības lielums, sarežģītība un vispārējais riska profils un tās pakalpojumu, darbību un operāciju veids, apmērs un sarežģītība.

4. Ne vairāk kā viens no atlasītajiem scenārijiem var nebūt draudu vadīts, un tas var būt balstīts uz nākotni vērstiem un potenciāli fiktīviem draudiem ar augstu prognozējošu, nojaušamu, oportūnistisku vai paredzamu vērtību, ņemot vērā nojaušamās norises apdraudējuma ainā attiecībā uz finanšu vienību.

Attiecībā uz apvienotām DVIT, neskarot scenārijus, kas tieši vērsti uz testēšanā iesaistīto finanšu vienību kritiski svarīgajām vai svarīgajām funkcijām, vismaz vienā scenārijā iekļauj trešās personas, kas sniedz IKT pakalpojumus, attiecīgās pamatā esošās IKT sistēmas, procesus un tehnoloģijas, ar kurām atbalsta darbības jomā ietilpstošo finanšu vienību kritiski svarīgās vai svarīgās funkcijas.

Ja tests ir kopīga DVIT, kurā iesaistīts IKT pakalpojumu sniedzējs, kas pieder vienai grupai, neskarot scenārijus, kas tieši vērsti uz testā iesaistīto finanšu vienību kritiski svarīgajām vai svarīgajām funkcijām, vismaz vienā scenārijā iekļauj IKT pakalpojumu sniedzēja, kurš pieder vienai grupai, attiecīgās pamatā esošās IKT sistēmas, procesus un tehnoloģijas, ar kurām atbalsta darbības jomā ietilpstošo finanšu vienību kritiski svarīgās vai svarīgās funkcijas.

5. Draudu izlūkdatu sniedzējs iesniedz kontroles komandai mērķorientētu draudu izlūkdatu ziņojumu, tostarp scenārijus, kas atlasīti saskaņā ar 3. un 4. punktu. Draudu izlūkdatu ziņojumā iekļauj III pielikumā izklāstīto informāciju.

6. Kontroles komanda mērķorientētu draudu izlūkdatu ziņojumu iesniedz testa pārvaldniekam apstiprināšanai. Ja mērķorientētais draudu izlūkdatu ziņojums ir pilnīgs un nodrošina rezultatīvas DVIT veikšanu, DVIT iestāde apstiprina mērķorientēto draudu izlūkdatu ziņojumu un par to informē kontroles komandas vadītāju.

11. pants

Testēšanas posms: sarkanās komandas tests

1. Pēc tam, kad DVIT iestāde ir apstiprinājusi mērķorientēto draudu izlūkdatu ziņojumu, testētāji sagatavo sarkanās komandas testēšanas plānu, kurā ietverta IV pielikumā izklāstītā informācija. Testētāji izmanto darbības jomas specifikācijas dokumentu un mērķorientēto draudu izlūkdatu ziņojumu kā pamatu uzbrukuma scenāriju izstrādei.

2. Testētāji apspriežas ar kontroles komandu, draudu izlūkdatu sniedzēju un testu pārvaldniekiem par sarkanās komandas testēšanas plānu, tostarp par saziņas, procesuālo un projekta pārvaldības kārtību, sagatavošanas pasākumiem un pielietošanas gadījumiem atbalsta aktivizēšanai, kā arī vienošanos par ziņošanu kontroles komandai un testu pārvaldniekiem.

3. Ja sarkanās komandas testēšanas plāns ir pilnīgs un nodrošina rezultatīvas DVIT veikšanu, kontroles komanda un DVIT iestāde apstiprina sarkanās komandas testēšanas plānu, un DVIT iestāde par to informē kontroles komandas vadītāju.

4. Pēc sarkanās komandas testēšanas plāna apstiprināšanas saskaņā ar 3. punktu testētāji DVIT veic sarkanās komandas aktīvās testēšanas posmā.

5. Sarkanās komandas aktīvās testēšanas posma ilgums ir samērīgs ar DVIT darbības jomu, ar DVIT iesaistīto finanšu vienību un trešo personu, kas sniedz IKT pakalpojumus, un vienai grupai piederošo IKT pakalpojumu sniedzēju lielumu, darbību, sarežģītību un skaitu, un jebkurā gadījumā tas ilgst vismaz 12 nedēļas. Uzbrukuma scenārijus var izpildīt secīgi vai vienlaikus. Kontroles komanda, draudu izlūkdatu sniedzējs, testētāji un testu pārvaldnieki vienojas par sarkanās komandas aktīvās testēšanas posma beigām.

6. Ja tiek nodrošināts, ka sarkanās komandas testēšanas plāns joprojām ir pilnīgs un ļauj veikt rezultatīvu DVIT, kontroles komandas vadītājs un testu pārvaldnieki apstiprina visas izmaiņas sarkanās komandas testēšanas plānā pēc tā apstiprināšanas, tostarp attiecībā uz grafiku, darbības jomu, mērķsistēmām vai atzīmēm.

7. Visā sarkanās komandas aktīvās testēšanas posmā testētāji vismaz reizi nedēļā ziņo kontroles komandai un testu pārvaldniekiem par progresu, kas panākts DVIT gaitā, un draudu izlūkdatu sniedzējs ir pieejams, lai sniegtu konsultācijas un papildu draudu izlūkdatus, ja to pieprasa kontroles komanda.

8. Kontroles komanda laikus nodrošina atbalstu, kas veidots, pamatojoties uz sarkanās komandas testēšanas plānu. Atbalstu var papildināt vai pielāgot pēc kontroles komandas un testu pārvaldnieku apstiprinājuma.

9. Ja kāds finanšu vienības vai attiecīgā gadījumā tās trešo personu, kas sniedz IKT pakalpojumus, vai IKT pakalpojumu sniedzēju, kuri pieder vienai grupai, darbinieks atklāj testēšanas darbības, kontroles komanda, apspriežoties ar testētājiem un neskarot 10. punktu, ierosina un iesniedz testu pārvaldniekiem apstiprināšanai pasākumus, kas ļauj turpināt DVIT, vienlaikus nodrošinot tās slepenību.

10. Izņēmuma apstākļos, kas rada risku, ka tiks ietekmēti dati, bojāti aktīvi un traucētas pašas finanšu vienības, tās trešo personu, kas sniedz IKT pakalpojumus, vai IKT pakalpojumu sniedzēju, kuri pieder vienai grupai, kritiski svarīgas vai svarīgas funkcijas, pakalpojumi vai darbības, vai radīti traucējumi tās darījumu partneriem vai finanšu nozarei, kontroles komanda var apturēt DVIT vai, ja DVIT turpināšana nav citādi iespējama un ja to iepriekš apstiprinājusi DVIT iestāde, turpināt DVIT, izmantojot to kā galējo līdzekli un veicot purpursarkanās komandas ierobežotu izmantošanas darbību. Purpursarkanās komandas ierobežotās izmantošanas darbības ilgumu nosaka tā, lai tiktu nodrošināts šā panta 5. punktā minētais sarkanās komandas aktīvās testēšanas posma minimālais ilgums, kas ir 12 nedēļas.

12. pants

Slēgšanas posms

1. Pēc sarkanās komandas aktīvās testēšanas posma beigām kontroles komandas vadītājs informē zilo komandu par to, ka tika veikta DVIT.

2. Četru nedēļu laikā pēc sarkanās komandas aktīvās testēšanas posma beigām testētāji iesniedz kontroles komandai sarkanās komandas testa ziņojumu, kurā ietverta V pielikumā izklāstītā informācija.

3. Kontroles komanda bez liekas kavēšanās iesniedz sarkanās komandas testa ziņojumu zilajai komandai un testu pārvaldniekiem.

Pēc testu pārvaldnieku pieprasījuma pirmajā daļā minētajā ziņojumā neiekļauj sensitīvu informāciju.

4. Pēc sarkanās komandas testa ziņojuma saņemšanas un ne vēlāk kā 10 nedēļas pēc sarkanās komandas aktīvās testēšanas posma beigām zilā komanda iesniedz kontroles komandai zilās komandas testa ziņojumu, kurā ietverta VI pielikumā izklāstītā informācija. Kontroles komanda bez liekas kavēšanās iesniedz zilās komandas testa ziņojumu testētājiem un testu pārvaldniekiem.

Pēc testu pārvaldnieku pieprasījuma pirmajā daļā minētajā ziņojumā neiekļauj sensitīvu informāciju.

5. Ne vēlāk kā 10 nedēļas pēc sarkanās komandas aktīvās testēšanas posma beigām zilā komanda un testētāji atkārto uzbrukuma un aizsardzības darbības, kas veiktas DVIT laikā. Kontroles komanda arī veic purpursarkanās komandas izmantošanas darbību par tematiem, ko kopīgi identificējusi zilā komanda un testētāji, pamatojoties uz testa laikā identificēto ievainojamību un attiecīgā gadījumā problēmām, kuras nebija iespējams testēt sarkanās komandas aktīvās testēšanas posmā.

6. Pēc atkārtošanas un purpursarkanās komandas izmantošanas darbības pabeigšanas kontroles komanda, zilā komanda, testētāji un draudu izlūkdatu sniedzēji savstarpēji sniedz atsauksmes par DVIT procesu. Testu pārvaldnieki var sniegt atsauksmes.

7. Pēc DVIT iestādes paziņojuma kontroles komandai par savu novērtējumu, ka zilās komandas testa ziņojumā un sarkanās komandas testa ziņojumā ir iekļauta V un VI pielikumā izklāstītā informācija, finanšu vienība astoņu nedēļu laikā iesniedz DVIT iestādei apstiprināšanai ziņojumu, kurā apkopoti attiecīgie DVIT konstatējumi, kā minēts Regulas (ES) 2022/2554 26. panta 6. punktā, un kurā ietverti VII pielikumā izklāstītie elementi.

Pēc DVIT iestādes pieprasījuma pirmajā daļā minētajā ziņojumā neiekļauj sensitīvu informāciju.

13. pants

Kļūdu novēršanas plāns

1. Pēc šīs regulas 12. panta 7. punktā minētā paziņojuma finanšu vienība astoņu nedēļu laikā iesniedz Regulas (ES) 2022/2554 26. panta 6. punktā minētos kļūdu novēršanas plānus un dokumentāciju DVIT un, ja tā atšķiras, finanšu vienības kompetentajai iestādei.

2. Šā panta 1. punktā minētajā kļūdu novēršanas plānā attiecībā uz katru konstatējumu, kas izdarīts saistībā ar DVIT, iekļauj:

a) identificēto trūkumu aprakstu;

b) aprakstu par ierosinātajiem kļūdu novēršanas pasākumiem un to prioritāšu noteikšanu un paredzamo pabeigšanu, tostarp attiecīgā gadījumā par pasākumiem, kas paredzēti, lai uzlabotu identificēšanas, aizsardzības, atklāšanas un reaģēšanas spējas;

c) pirmcēloņa analīzi;

d) finanšu vienības personālu vai funkcijas, kas atbildīgas par ierosināto kļūdu novēršanas pasākumu vai uzlabojumu īstenošanu;

e) riskiem, kas saistīti ar b) apakšpunktā minēto pasākumu neīstenošanu, un attiecīgā gadījumā riskiem, kas saistīti ar šādu pasākumu īstenošanu.

14. pants

Apliecinājums

1. Regulas (ES) 2022/2554 26. panta 7. punktā minētajā apliecinājumā iekļauj VIII pielikumā izklāstīto informāciju.

2. Ja DVIT ir iesaistītas vairākas DVIT iestādes, vadošā DVIT iestāde finanšu vienībām, kurām veic testēšanu, iesniedz Regulas (ES) 2022/2554 26. panta 7. punktā minēto apliecinājumu.

15. pants

Iekšējo testētāju izmantošana

1. Finanšu vienības izstrādā visus turpmāk minētos noteikumus iekšējo testētāju izmantošanai:

a) rīcībpolitikas izstrāde un īstenošana attiecībā uz iekšējo testētāju pārvaldību DVIT;

b) pasākumi, ar kuriem nodrošina, ka iekšējo testētāju izmantošana DVIT veikšanai negatīvi neietekmē finanšu vienības vispārējās aizsardzības vai noturības spējas attiecībā uz incidentiem, kas saistīti ar IKT, vai būtiski neietekmē ar IKT saistītiem uzdevumiem veltītu resursu pieejamību DVIT laikā;

c) pasākumi, ar kuriem nodrošina, ka iekšējiem testētājiem ir pietiekami resursi un spējas, lai veiktu DVIT.

Šā punkta a) apakšpunktā minētā rīcībpolitika:

a) ietver kritērijus iekšējo testētāju piemērotības, kompetences, iespējamo interešu konfliktu novērtēšanai, un tajā precizēti pārvaldības pienākumi testēšanas procesā;

b) ir dokumentēta un tiek periodiski pārskatīta;

c) nodrošina, ka iekšējā testēšanas komandā ir testa vadītājs un vismaz divi papildu locekļi;

d) paredz, ka visi testēšanas komandas locekļi iepriekšējos 12 mēnešus ir bijuši nodarbināti finanšu vienībā vai pie IKT pakalpojumu sniedzēja, kurš pieder vienai grupai;

e) ietver noteikumus iekšējo testētāju apmācībai par to, kā veikt ielaušanās testēšanu un sarkanās komandas testēšanu.

2. Ja DVIT iestāde apstiprina iekšējo testētāju izmantošanu saskaņā ar Regulas (ES) 2022/2554 27. panta 2. punkta a) apakšpunktu, DVIT iestāde ņem vērā šīs regulas 7. panta 1. punktā noteiktās prasības.

3. Izmantojot iekšējos testētājus, finanšu vienība nodrošina, ka šāda izmantošana ir minēta šādos dokumentos:

a) informācijā par testa uzsākšanu, kas minēta 9. pantā;

b) sarkanās komandas testa ziņojumā, kas minēts 12. panta 2. punktā;

c) Regulas (ES) 2022/2554 26. panta 6. punktā minētajā ziņojumā, kurā apkopoti attiecīgie DVIT konstatējumi.

4. Testētājus, ko nodarbina IKT pakalpojumu sniedzējs, kurš pieder vienai grupai, uzskata par finanšu vienības iekšējiem testētājiem.

16. pants

Sadarbība un savstarpēja atzīšana

1. DVIT veikšanas nolūkos attiecībā uz finanšu vienību, kas sniedz pakalpojumus vairāk nekā vienā dalībvalstī, tostarp ar filiāles starpniecību, tās DVIT iestāde:

a) nosaka, kuras DVIT iestādes uzņēmējās dalībvalstīs tiks iesaistītas, ņemot vērā to, vai uzņēmējās dalībvalstīs tiek veikta viena vai vairākas kritiski svarīgas vai svarīgas funkcijas vai tās tiek kopīgi izmantotas tajās;

b) saskaņā ar a) apakšpunktu noteiktās DVIT iestādes informē par lēmumu veikt DVIT testu finanšu vienībai;

c) ja vien DVIT iestādes nevienojas citādi, finanšu vienības DVIT iestāde vada DVIT.

Uzņēmēju dalībvalstu DVIT iestādes 20 darbdienu laikā pēc tam, kad saņemta informācija par DVIT turpmāku veikšanu, var vai nu paust interesi sekot DVIT novērotāju statusā, vai norīkot testa pārvaldnieku dalībai DVIT. Vadošā DVIT iestāde visām DVIT iestādēm, kas DVIT darbojas novērotāju statusā, iesniedz darbības jomas specifikācijas dokumentu, testa kopsavilkuma ziņojumu, kļūdu novēršanas plānu un apliecinājumu.

Vadošā DVIT iestāde koordinē visas iesaistītās DVIT iestādes visā testa gaitā un pieņem visus lēmumus, kas vajadzīgi, lai pienācīgi un rezultatīvi veiktu DVIT. Vadošā DVIT iestāde var noteikt maksimālo iesaistīto DVIT iestāžu skaitu, ja pretējā gadījumā varētu tikt apdraudēta rezultatīva DVIT veikšana.

2. Ja finanšu vienība izmanto to pašu vienā grupā ietilpstošu IKT pakalpojumu sniedzēju, ko izmanto finanšu vienības, kas iedibinātas citās dalībvalstīs, vai ja tā pieder grupai un kopīgi izmanto IKT sistēmas ar tās pašas grupas finanšu vienībām, kas iedibinātas citās dalībvalstīs, finanšu vienības DVIT iestāde sazinās ar citu to finanšu vienību DVIT iestādēm, kuras izmanto to pašu vienā grupā ietilpstošu IKT pakalpojumu sniedzēju vai kuras grupas ietvaros kopīgi izmanto IKT sistēmas, un kopā ar tām novērtē kopīgas DVIT veikšanas iespējamību un piemērotību attiecībā uz tām. Priekšroka dodama kopīgai DVIT, nevis atsevišķai DVIT, ja tās rezultātā finanšu vienības un DVIT iestādes var samazināt izmaksas un resursus, ar noteikumu, ka netiek apdraudēta testēšanas stabilitāte un efektivitāte.

3. Kopīgas DVIT nolūkos:

a) finanšu vienību DVIT iestādes vienojas par to, kura finanšu vienība tiks izraudzīta, lai veiktu DVIT, ņemot vērā grupas struktūru un testa efektivitāti;

b) saskaņā ar a) apakšpunktu izraudzītās finanšu vienības DVIT iestāde vada DVIT, ja vien kopīgajā DVIT iesaistīto finanšu vienību DVIT iestādes nav vienojušās citādi;

c) finanšu vienību DVIT iestādes, kas nav izraudzītās finanšu vienības DVIT iestāde, kura vada kopīgo DVIT, var vai nu paust interesi sekot DVIT novērotāju statusā, vai norīkot testa pārvaldnieku minētajai DVIT.

Vadošā DVIT iestāde koordinē visas kopīgajā DVIT iesaistītās DVIT iestādes un pieņem visus lēmumus, kas vajadzīgi, lai pienācīgi un rezultatīvi veiktu kopīgo DVIT.

4. Ja finanšu vienība plāno veikt apvienotu DVIT, kā minēts Regulas (ES) 2022/2554 26. panta 4. punktā, iespējams, iesaistot finanšu vienības, kas iedibinātas citās dalībvalstīs, tās DVIT iestāde sazinās ar citu finanšu vienību DVIT iestādēm un kopā ar tām novērtē iespēju un piemērotību veikt apvienotu DVIT attiecībā uz tām saskaņā ar Regulas (ES) 2022/2554 26. panta 4. punktu.

5. Kā noteikts Regulas (ES) 2022/2554 26. panta 4. punktā, apvienotas DVIT veikšanas nolūkos:

a) finanšu vienību DVIT iestādes vienojas par to, kura finanšu vienība tiks izraudzīta vadīt apvienoto DVIT, ņemot vērā IKT pakalpojumus, ko finanšu vienībām sniedz trešā persona, kas sniedz IKT pakalpojumus, un par testa efektivitāti;

b) saskaņā ar a) apakšpunktu izraudzītās finanšu vienības DVIT iestāde vada DVIT, ja vien apvienotajā DVIT iesaistīto finanšu vienību DVIT iestādes nav vienojušās citādi;

c) finanšu vienību DVIT iestādes, kas nav izraudzītās finanšu vienības DVIT iestāde, kura vada apvienoto DVIT, var vai nu paust interesi sekot DVIT novērotāju statusā, vai norīkot testa pārvaldnieku minētajai DVIT.

Vadošā DVIT iestāde koordinē visas apvienotajā DVIT iesaistītās DVIT iestādes un pieņem visus lēmumus, kas vajadzīgi, lai pienācīgi un rezultatīvi veiktu apvienoto DVIT.

6. Ja attiecībā uz finanšu vienību, kurai ir pienākums veikt DVIT, tās DVIT iestāde atšķiras no tās Regulas (ES) 2022/2554 46. pantā minētās kompetentās iestādes, minētās iestādes apmainās ar visu attiecīgo informāciju par visiem ar DVIT saistītajiem jautājumiem DVIT veikšanas vai savu pienākumu veikšanas saskaņā ar minēto regulu nolūkos.

17. 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, 2025. gada 13. februārī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

Projekta nolikuma saturs (9. panta 2. punkta a) apakšpunkts)

Informācijas vienība	Prasītā informācija
Par projekta plānu atbildīgā persona, t. i., kontroles komandas vadītājs	Vārds, uzvārds Kontaktinformācija
Testētāji	☐ Iekšējie ☐ Ārējie ☐ Abi
Saziņas kanāli, kas atlasīti saskaņā ar 9. panta 2. punkta d) apakšpunktu un 9. panta 4. punkta a) apakšpunktu, tostarp: a) izmantojamā e-pasta šifrēšana; b) izmantojamās tiešsaistes datu telpas; c) izmantojamā tūlītējā ziņapmaiņa.	
DVIT kodētais nosaukums	
Ja tādas ir, kritiski svarīgas vai svarīgas funkcijas, ko finanšu vienība veic citās dalībvalstīs	1. Citā dalībvalstī veikto kritiski svarīgo vai svarīgo funkciju saraksts. 2. Attiecībā uz katru kritiski svarīgu vai svarīgu funkciju – norāde par dalībvalsti vai dalībvalstīm, kurās tās tiek veiktas.
Ja tādas ir, kritiski svarīgas vai svarīgas funkcijas, ko atbalsta trešās personas, kas sniedz IKT pakalpojumus	3. Tādu kritiski svarīgu vai svarīgu funkciju saraksts, kuras atbalsta trešās personas, kas sniedz IKT pakalpojumus. 4. Attiecībā uz katru funkciju – trešās personas, kas sniedz IKT pakalpojumus, identifikācija.
Paredzamais pabeigšanas termiņš attiecībā uz:	
1) sagatavošanas posmu saskaņā ar 9. pantu	gggg-mm-dd
2) testēšanas posmu saskaņā ar 10. un 11. pantu	gggg-mm-dd
3) slēgšanas posmu saskaņā ar 12. pantu	gggg-mm-dd
4) kļūdu novēršanas plānu saskaņā ar 13. pantu	gggg-mm-dd

II PIELIKUMS

Darbības jomas specifikācijas dokumenta saturs (9. panta 6. punkts)

1. Darbības jomas specifikācijas dokumentā iekļauj visu finanšu vienības identificēto kritiski svarīgo vai svarīgo funkciju sarakstu.

2. Attiecībā uz katru identificēto kritiski svarīgo vai svarīgo funkciju iekļauj šādu informāciju:
   a) ja kritiski svarīgā vai svarīgā funkcija nav iekļauta DVIT darbības jomā, paskaidrojums par iemesliem, kuru dēļ tā nav iekļauta;
   b) ja kritiski svarīgā vai svarīgā funkcija ir iekļauta DVIT darbības jomā:
      i) paskaidrojums par tās iekļaušanas iemesliem;
      ii) identificētā(-ās) IKT sistēma(-as), ar kurām atbalsta minēto kritiski svarīgo vai svarīgo funkciju;
      iii) attiecībā uz katru identificēto IKT sistēmu:
         1) vai tā ir nodota ārpakalpojumā, un, ja tā ir, trešās personas, kas sniedz IKT pakalpojumus, nosaukums;
         2) jurisdikcijas, kurās izmanto IKT sistēmu;
         3) sākotnējās(-o) atzīmes(-ju) augsta līmeņa apraksts, kurā norāda, uz kuru konfidencialitātes, integritātes, autentiskuma vai pieejamības drošības aspektu katra atzīme attiecas.

III PIELIKUMS

Mērķorientētā draudu izlūkdatu ziņojuma saturs (10. panta 5. punkts)

Mērķorientētajā draudu izlūkdatu ziņojumā ietver informāciju par visu turpmāk minēto.

1. Izlūkdatu pētījuma vispārējā darbības joma, tostarp vismaz šādi aspekti:
   a) darbības jomā ietilpstošas kritiski svarīgas vai svarīgas funkcijas;
   b) to ģeogrāfiskā atrašanās vieta;
   c) izmantotā oficiālā ES valoda;
   d) attiecīgās trešās personas, kas sniedz IKT pakalpojumus;
   e) laika periods, kurā tiek apkopots pētījums.
2. Vispārējais novērtējums par to, kādus konkrētus praktiskus izlūkdatus var atrast par finanšu vienību, tostarp:
   a) darbinieku lietotājvārdi un paroles;
   b) līdzīgi domēni, kurus var sajaukt ar finanšu vienības oficiālajiem domēniem;
   c) tehniskā izlūkošana: ievainojama vai izmantojama programmatūra, sistēmas un tehnoloģijas;
   d) ar finanšu vienību saistīta informācija, ko darbinieki ievietojuši internetā un ko varētu izmantot uzbrukuma nolūkos;
   e) informācija pārdošanai tumšajā tīmeklī;
   f) jebkāda cita būtiska informāciju, kas pieejama internetā vai publiskajos tīklos;
   g) attiecīgā gadījumā informācija par fizisku mērķorientēšanu, tostarp veidiem, kā piekļūt finanšu vienības telpām.
3. Draudu izlūkdatu analīze, ņemot vērā vispārējo apdraudējuma ainu un finanšu vienības īpašo situāciju, tostarp vismaz:
   a) ģeopolitiskā vide;
   b) ekonomiskā vide;
   c) tehnoloģiskās tendences un citas tendences, kas saistītas ar darbībām finanšu pakalpojumu nozarē.
4. To ļaunprātīgo personu draudu profili (konkrēts indivīds/grupa vai vispārēja kategorija), kas var vērsties pret finanšu vienību, tostarp pret tām finanšu vienības sistēmām, kuras ļaunprātīgas personas, visticamāk, varētu apdraudēt vai vērsties pret tām, potenciālās mērķorientēšanas iespējamā motivācija, nolūks un pamatojums un uzbrucēju iespējamais darbības veids.
5. Apdraudējuma scenāriji: vismaz trīs pilnīgi apdraudējuma scenāriji tiem draudu profiliem, kuri noteikti saskaņā ar 4. punktu un kuriem ir visaugstākais apdraudējuma smaguma vērtējums. Apdraudējuma scenārijos pilnīgi apraksta uzbrukuma ceļu un ietver vismaz:
   a) vienu scenāriju, kas ietver, bet neaprobežojas ar apdraudētu pakalpojumu pieejamību;
   b) vienu scenārijs, kas ietver, bet neaprobežojas ar apdraudētu datu integritāti;
   c) vienu scenāriju, kas ietver, bet neaprobežojas ar apdraudētu informācijas konfidencialitāti.
6. Attiecīgā gadījumā 10. panta 4. punktā minētā scenārija, kas nav draudu vadīts, apraksts.

IV PIELIKUMS

Sarkanās komandas testēšanas plāna saturs (11. panta 1. punkts)

Sarkanās komandas testēšanas plānā ietver informāciju par visu turpmāk minēto:

a) saziņas kanāli un procedūras;

b) taktikas, paņēmieni un procedūras, kas ir atļautas un nav atļautas izmantošanai uzbrukumā, tostarp sociālās inženierijas ētiskās robežas;

c) riska pārvaldības pasākumi, kas jāievēro testētājiem;

d) katra scenārija apraksts, tostarp:

   i) simulētais apdraudējuma dalībnieks;

   ii) tā nodomi, motivācija un mērķi;

   iii) mērķa funkcija(-as) un atbalstošā(-ās) IKT sistēma(-as);

   iv) mērķorientēti konfidencialitātes, integritātes, pieejamības un autentiskuma aspekti;

   v) atzīmes;

e) detalizēts apraksts par katru paredzamo uzbrukuma ceļu, tostarp priekšnosacījumi un iespējamais atbalsts, ko kontroles komanda sniegs, tostarp tā sniegšanas un iespējamās izmantošanas termiņi;

f) to sarkanās komandas izmantošanas darbību plānošana, ko testētājs veic visā testēšanas posmā, iekļūstot finanšu vienību IKT sistēmās, pārvietojoties caur IKT sistēmām un galu galā veicot darbības attiecībā uz mērķi, kā arī beigās izkļūstot no IKT sistēmām (iekļūšanas, pārvietošanās, izkļūšanas posmi), tostarp laika plāns katra scenārija izpildei vismaz sadalījumā pa trim posmiem;

g) finanšu vienību infrastruktūras īpatnības, kas jāņem vērā testēšanas laikā;

h) papildu informācija vai citi resursi, kas testētājiem vajadzīgi scenāriju izpildei, ja tādi ir.

V PIELIKUMS

Sarkanās komandas testa ziņojuma saturs (12. panta 2. punkts)

Sarkanās komandas testa ziņojumā ietver informāciju par vismaz visu turpmāk minēto:

a) informāciju par veikto uzbrukumu, tostarp:

   i) kritiski svarīgās vai svarīgās funkcijas, pret kurām tika vērsts uzbrukums, un identificētās IKT sistēmas, procesi un tehnoloģijas, ar kurām atbalsta kritiski svarīgo vai svarīgo funkciju īstenošanu, kā noteikts sarkanās komandas testēšanas plānā;

   ii) katra scenārija kopsavilkumu;

   iii) sasniegtās un nesasniegtās atzīmes;

   iv) sekmīgi un nesekmīgi veiktos uzbrukuma ceļus;

   v) sekmīgi un nesekmīgi izmantotās taktikas, paņēmienus un procedūras;

   vi) novirzes no sarkanās komandas testēšanas plāna, ja tādas ir;

   vii) piešķirto atbalstu, ja tāds ir;

b) visas darbības, par kurām testētāji ir informēti un kuras veikusi zilā komanda, lai rekonstruētu uzbrukumu un mazinātu tā sekas;

c) atklāto ievainojamību un citus konstatējumus, tostarp:

   i) ievainojamības un citu konstatējumu aprakstu, tostarp to kritiskumu;

   ii) sekmīgu uzbrukumu pamatcēloņu analīzi;

   iii) ieteikumus kļūdu novēršanai, tostarp norādi par kļūdu novēršanas prioritāti.

VI PIELIKUMS

Zilās komandas testa ziņojuma saturs (12. panta 4. punkts)

Zilās komandas testa ziņojumā ietver informāciju par vismaz visu turpmāk minēto:

1) attiecībā uz katru uzbrukuma posmu, ko testētāji aprakstījuši sarkanās komandas testa ziņojumā:
   a) atklāto uzbrukuma darbību saraksts;
   b) reģistra ieraksti, kas atbilst šiem atklājumiem;
2) testētāju konstatējumu un ieteikumu novērtējums;
3) zilās komandas apkopotie pierādījumi par testētāju uzbrukumu;
4) testētāju veikto veiksmīgo uzbrukumu pamatcēloņu analīze, ko izstrādājusi zilā komanda;
5) saraksts ar gūtajām atziņām un identificētajām uzlabojumu iespējām;
6) to tematu saraksts, kuriem jāpievēršas purpursarkanās komandas izmantošanas laikā.

VII PIELIKUMS

Sīkāka informācija par Regulas (ES) 2022/2554 26. panta 6. punktā minēto ziņojumu, kurā apkopoti attiecīgie DVIT konstatējumi

Testa kopsavilkuma ziņojumā ietver informāciju par vismaz visu turpmāk minēto:

a) iesaistītās personas;

b) projekta plāns;

c) apstiprinātā darbības joma, tostarp pamatojums kritiski svarīgu vai svarīgu funkciju un tādu identificēto IKT sistēmu, procesu un tehnoloģiju iekļaušanai vai izslēgšanai, ar kurām atbalsta kritiski svarīgās vai svarīgās funkcijas, uz kurām attiecas DVIT;

d) atlasītie scenāriji un jebkādas būtiskas novirzes no mērķorientētā draudu izlūkdatu ziņojuma;

e) īstenotie uzbrukuma ceļi un izmantotās taktikas, paņēmieni un procedūras;

f) iegūtās un neiegūtās atzīmes;

g) novirzes no sarkanās komandas testēšanas plāna, ja tādas ir;

h) zilās komandas atklāšana, ja tāda ir;

i) purpursarkanās komandas izmantošana testēšanas posmā, ja to veic, un ar to saistītie apstākļi;

j) izmantotais atbalsts, ja tāds ir;

k) veiktie riska pārvaldības pasākumi;

l) identificētā ievainojamība un citi konstatējumi, tostarp to kritiskums;

m) sekmīgu uzbrukumu pamatcēloņu analīze;

n) augsta līmeņa plāns kļūdu novēršanai, sasaistot ievainojamību un citus konstatējumus, to pamatcēloņi un kļūdu novēršanas prioritāte;

o) gūtās atziņas no saņemtajām atsauksmēm.

VIII PIELIKUMS

Sīkāka informācija par Regulas (ES) 2022/2554 26. panta 7. punktā minēto DVIT apliecinājumu

Apliecinājumā ietver vismaz visu turpmāk minēto informāciju:

a) par veikto DVIT:

   i) DVIT sākuma un beigu datums;

   ii) kritiski svarīgā vai svarīgā funkcija DVIT darbības jomā;

   iii) attiecīgā gadījumā informācija par kritiski svarīgām vai svarīgām funkcijām testa darbības jomā, attiecībā uz kurām DVIT netika veikta;

   iv) attiecīgā gadījumā citas finanšu vienības, kas bija iesaistītas DVIT;

   v) attiecīgā gadījumā trešās personas, kas sniedz IKT pakalpojumus un ir piedalījušās DVIT;

   vi) attiecībā uz testētājiem:

      1) vai tika izmantoti iekšējie testētāji;

      2) vai finanšu vienība ir izmantojusi 5. panta 3. punkta otro daļu;

   vii) sarkanās komandas aktīvās testēšanas posma ilgums kalendārajās dienās;

b) ja DVIT ir iesaistītas vairākas DVIT iestādes – pārējās DVIT iestādes un kādā statusā;

c) to dokumentu saraksts, kurus DVIT iestāde pārbaudījusi apliecinājuma vajadzībām.