2024/1774

25.6.2024

KOMISSION DELEGOITU ASETUS (EU) 2024/1774,

annettu 13 päivänä maaliskuuta 2024,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 täydentämisestä TVT-riskinhallintavälineitä, -menetelmiä, -menettelyitä ja -politiikkatoimia sekä yksinkertaistettua TVT-riskinhallintajärjestelmää koskevilla teknisillä sääntelystandardeilla

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta 14 päivänä joulukuuta 2022 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ([1]) ja erityisesti sen 15 artiklan neljännen alakohdan ja 16 artiklan 3 kohdan neljännen alakohdan,

sekä katsoo seuraavaa:

(1) Asetuksen (EU) 2022/2554 soveltamisalaan kuuluu laaja kirjo kooltaan, rakenteeltaan, sisäiseltä organisaatioltaan sekä toiminnan luonteeltaan ja laajuudeltaan erilaisia finanssiyhteisöjä, joihin liittyy näin ollen enemmän tai vähemmän monimutkaisuutta ja riskitekijöitä. Jotta varmistetaan, että tämä moninaisuus otetaan asianmukaisesti huomioon, kaikkien TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä sekä yksinkertaistettua TVT-riskinhallintajärjestelmää koskevien vaatimusten olisi oltava oikeassa suhteessa finanssiyhteisöjen kokoon, rakenteeseen, sisäiseen organisaatioon, luonteeseen ja monimutkaisuuteen sekä niihin liittyviin riskeihin.

(2) Samasta syystä asetuksen (EU) 2022/2554 soveltamisalaan kuuluvilla finanssiyhteisöillä olisi oltava tietty joustovara sen suhteen, miten ne noudattavat TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä sekä yksinkertaistettua TVT-riskinhallintajärjestelmää koskevia vaatimuksia. Tästä syystä finanssiyhteisöjen olisi voitava käyttää kyseisistä vaatimuksista johtuvien dokumentaatiovaatimusten täyttämiseen mitä tahansa niillä jo olevaa dokumentaatiota. Tästä seuraa, että erityisten TVT-turvallisuutta koskevien toimintaperiaatteiden laatimista, dokumentointia ja täytäntöönpanoa olisi vaadittava vain tiettyjen olennaisten osatekijöiden osalta ottaen huomioon muun muassa alan johtavat käytännöt ja standardit. Jotta voidaan ottaa huomioon täytäntöönpanoon liittyvät erityiset tekniset näkökohdat, on lisäksi tarpeen laatia, dokumentoida ja ottaa käyttöön TVT-turvallisuutta koskevat toimintaperiaatteet, joilla katetaan tietyt täytäntöönpanoon liittyvät tekniset näkökohdat, mukaan lukien kapasiteetin ja suorituskyvyn hallinta, haavoittuvuuksien ja korjauspäivitysten hallinta, tietojen ja järjestelmän turvallisuus sekä lokikirjanpito.

(3) Jotta voidaan varmistaa tämän asetuksen II osaston I luvussa tarkoitettujen TVT-turvallisuutta koskevien toimintaperiaatteiden, menettelyjen, protokollien ja välineiden asianmukainen täytäntöönpano ajan mittaan, on tärkeää, että finanssiyhteisöt osoittavat ja ylläpitävät asianmukaisesti TVT-turvallisuuteen liittyviä rooleja ja vastuita ja että ne vahvistavat seuraukset TVT-turvallisuutta koskevien toimintaperiaatteiden tai menettelyjen noudattamatta jättämisestä.

(4) Eturistiriitojen riskin lieventämiseksi finanssiyhteisöjen olisi varmistettava tehtävien eriyttäminen, kun ne määrittelevät TVT-rooleja ja -vastuita.

(5) Joustavuuden varmistamiseksi ja finanssiyhteisöjen valvontakehyksen yksinkertaistamiseksi finanssiyhteisöjä ei tulisi vaatia laatimaan erityisiä säännöksiä seurauksista, joita aiheutuu tämän asetuksen II osaston I luvussa tarkoitettujen TVT-turvallisuutta koskevien toimintaperiaatteiden, menettelyjen ja protokollien noudattamatta jättämisestä, jos tällaiset säännökset on jo vahvistettu muissa toimintaperiaatteissa tai menettelyissä.

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

(6) Dynaamisessa ympäristössä, jossa TVT-riskit kehittyvät jatkuvasti, on tärkeää, että finanssiyhteisöt laativat TVT-turvallisuutta koskevat toimintaperiaatteensa johtavien käytäntöjen ja tapauksen mukaan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ([2]) 2 artiklan 1 alakohdassa määriteltyjen standardien pohjalta. Näin tämän asetuksen II osastossa tarkoitetut finanssiyhteisöt pysyvät ajan tasalla muuttuvasta ympäristöstä ja voivat valmistautua muutoksiin.

(7) Digitaalisen häiriönsietokykynsä varmistamiseksi tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi osana TVT-turvallisuutta koskevia toimintaperiaatteitaan, menettelyjään, protokolliaan ja välineitään kehitettävä ja pantava täytäntöön TVT-omaisuudenhallintaperiaatteet, valmiuksien ja suorituskyvyn hallintamenettelyt sekä TVT-toimia koskevat toimintaperiaatteet ja menettelyt. Toimintaperiaatteet ja menettelyt ovat tarpeen, jotta voidaan varmistaa TVT-omaisuuden tilan seuranta sen koko elinkaaren ajan ja jotta omaisuutta käytetään ja ylläpidetään tehokkaasti (TVT-omaisuudenhallinta). Toimintaperiaatteilla ja menettelyillä olisi myös varmistettava TVT-järjestelmien toiminnan optimointi ja se, että TVT-järjestelmien suorituskyky ja kapasiteetti vastaavat vakiintuneita liiketoiminta- ja tietoturvatavoitteita (kapasiteetin ja suorituskyvyn hallinta). Lisäksi toimintaperiaatteilla ja menettelyillä olisi varmistettava TVT-järjestelmien tehokas ja sujuva päivittäinen hallinnointi ja toiminta (TVT-toimet) ja minimoitava riski tietojen luottamuksellisuuden, eheyden ja saatavuuden heikkenemisestä. Toimintaperiaatteet ja menettelyt ovat näin ollen tarpeen verkkojen turvallisuuden varmistamiseksi, riittävien suojatoimien tarjoamiseksi tunkeutumista ja tietojen väärinkäyttöä vastaan sekä tietojen saatavuuden, aitouden, eheyden ja luottamuksellisuuden turvaamiseksi.

(8) Jotta voidaan varmistaa aiemman sukupolven TVT-järjestelmiin liittyvien riskien asianmukainen hallinta, finanssiyhteisöjen olisi kirjattava kolmansien osapuolten TVT-tukipalvelujen päättymispäivät ja seurattava niitä. Kun otetaan huomioon tietojen luottamuksellisuuden, eheyden ja saatavuuden heikkenemisen mahdolliset vaikutukset, finanssiyhteisöjen olisi keskityttävä liiketoiminnan kannalta kriittisiin TVT-omaisuuseriin tai -järjestelmiin, kun ne kirjaavat ja seuraavat kyseisiä päättymispäiviä.

(9) Salaustekniikkaa hyödyntävällä valvonnalla voidaan varmistaa tietojen saatavuus, aitous, eheys ja luottamuksellisuus. Tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi sen vuoksi määritettävä tällainen valvonta ja toteutettava sitä riskiperusteista lähestymistapaa noudattaen. Tätä varten finanssiyhteisöjen olisi salattava tiedot levossa, siirtämisen aikana tai tarvittaessa käsittelyn aikana kaksivaiheisen prosessin eli tietojen luokittelun ja kattavan TVT-riskinarvioinnin tulosten perusteella. Koska tietojen salaaminen käsittelyn aikana on monimutkaista, tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi salattava tiedot käsittelyn aikana vain, jos se on asianmukaista TVT-riskinarvioinnin tulosten perusteella. Tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi kuitenkin voitava suojata tietojen luottamuksellisuutta, eheyttä ja saatavuutta käsittelyn aikana muiden TVT-turvallisuutta koskevien toimenpiteiden avulla, jos tietojen salaaminen käsittelyn aikana on mahdotonta tai liian monimutkaista. Salaustekniikoiden nopean teknologisen kehityksen vuoksi tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi pysyttävä ajan tasalla salausanalyysin kehityksestä ja tarkasteltava alan johtavia käytäntöjä ja standardeja. Tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi sen vuoksi noudatettava riskien lieventämiseen ja seurantaan perustuvaa joustavaa lähestymistapaa salaukseen liittyvien uhkien, myös kvanttilaskennan kehittymisestä aiheutuvien uhkien, dynaamisen toimintaympäristön käsittelemiseksi.

(10) TVT-toimien turvallisuus ja operatiiviset toimintaperiaatteet, menettelyt, protokollat ja välineet ovat olennaisen tärkeitä tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi. Yksi keskeinen näkökohta on TVT-tuotantoympäristöjen täydellinen erottaminen TVT-järjestelmän kehitys- ja testausympäristöistä ja muista tuotannon ulkopuolisista ympäristöistä. Eriyttämisen olisi oltava tärkeä TVT-turvatoimenpide, jolla ehkäistään tuotantoympäristössä tietojen tahaton ja luvaton käyttö, muuttaminen ja poistaminen, jotka voisivat aiheuttaa merkittäviä häiriöitä tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen liiketoiminnalle. Ottaen kuitenkin huomioon nykyiset TVT-järjestelmien kehittämiskäytännöt finanssiyhteisöjen olisi poikkeuksellisissa olosuhteissa voitava suorittaa testejä tuotantoympäristöissä edellyttäen, että ne perustelevat tällaisen testauksen ja saavat vaaditun hyväksynnän.

([2]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta (EUVL L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Tieto- ja viestintätekniikan nopea kehitys, TVT-haavoittuvuustekijät ja kyberuhat edellyttävät ennakoivaa ja kattavaa lähestymistapaa TVT-haavoittuvuuksien tunnistamiseen, arviointiin ja korjaamiseen. Ilman tällaista lähestymistapaa finanssiyhteisöt, niiden asiakkaat, käyttäjät tai vastapuolet voivat altistua vakavasti riskeille, jotka vaarantaisivat niiden digitaalisen häiriönsietokyvyn, niiden verkkojen turvallisuuden sekä sellaisten tietojen saatavuuden, aitouden, eheyden ja luottamuksellisuuden, joita TVT-turvallisuutta koskevilla toimintaperiaatteilla ja menettelyillä olisi suojattava. Tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi sen vuoksi tunnistettava ja korjattava TVT-ympäristönsä haavoittuvuudet, ja sekä finanssiyhteisöjen että niiden TVT-palveluntarjoajana olevien kolmansien osapuolten olisi noudatettava johdonmukaista, läpinäkyvää ja vastuullista haavoittuvuuden hallintakehystä. Samasta syystä finanssiyhteisöjen olisi seurattava TVT-haavoittuvuuksia luotettavien resurssien ja automatisoitujen välineiden avulla ja varmistettava, että TVT-palveluntarjoajana olevat kolmannet osapuolet reagoivat nopeasti tarjottujen TVT-palvelujen haavoittuvuuksiin.

(12) Korjauspäivitysten hallinnan olisi oltava keskeinen osa niitä TVT-turvallisuutta koskevia toimintaperiaatteita ja menettelyjä, joilla on määrä testauksen ja valvotussa ympäristössä tapahtuvan käyttöönoton avulla korjata havaitut haavoittuvuudet ja estää korjauspäivitysten asentamisesta aiheutuvat häiriöt.

(13) Jotta voidaan varmistaa oikea-aikainen ja läpinäkyvä tiedottaminen mahdollisista turvallisuusuhkista, jotka voivat vaikuttaa finanssiyhteisöön ja sen sidosryhmiin, finanssiyhteisöjen olisi otettava käyttöön menettelyt TVT-haavoittuvuuksista ilmoittamiseksi vastuullisesti asiakkaille, vastapuolille ja suurelle yleisölle. Kyseisiä menettelyjä vahvistaessaan finanssiyhteisöjen olisi otettava huomioon erilaisia tekijöitä, kuten haavoittuvuuden vakavuus, haavoittuvuuden mahdollinen vaikutus sidosryhmiin ja korjaus- tai lieventämistoimenpiteiden käyttövalmius.

(14) Käyttöoikeuksien myöntämisen mahdollistamiseksi tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi otettava käyttöön tehokkaita toimenpiteitä, joilla varmistetaan niiden henkilöiden ja järjestelmien yksilöllinen tunnistaminen, joilla on pääsy finanssiyhteisön tietoihin. Jos näin ei tehdä, finanssiyhteisöt altistuisivat mahdolliselle luvattomalle tietoihin pääsylle, tietoturvaloukkauksille ja petolliselle toiminnalle, mikä vaarantaisi arkaluonteisten rahoitustietojen luottamuksellisuuden, eheyden ja saatavuuden. Vaikka yleisen tai yhteiskäyttöisen tilin käyttö olisi poikkeuksellisesti sallittava finanssiyhteisöjen täsmentämissä olosuhteissa, finanssiyhteisöjen olisi varmistettava, että vastuuvelvollisuus kyseisten tilien kautta toteutetuista toimista toteutuu. Ilman tätä suojatoimenpidettä mahdolliset pahantahtoiset toimijat voisivat haitata tutkinta- ja korjaavia toimenpiteitä, minkä vuoksi finanssiyhteisöt voisivat jäädä alttiiksi havaitsemattomille vihamielisille toimille ja niille voisi koitua seuraamuksia sääntöjen noudattamatta jättämisestä.

(15) Jotta voidaan hallita TVT-ympäristöjen nopeaa kehitystä, tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi pantava täytäntöön vankat TVT-projektihallinnan periaatteet ja menettelyt tietojen saatavuuden, aitouden, eheyden ja luottamuksellisuuden suojaamiseksi. TVT-projektihallinnan periaatteissa ja menettelyissä olisi määritettävä tekijät, jotka ovat tarpeen TVT-projektien menestyksekkään hallinnoinnin kannalta, mukaan lukien finanssiyhteisön TVT-järjestelmien muutokset, hankinnat, ylläpito ja kehittäminen, riippumatta finanssiyhteisön valitsemasta TVT-projektinhallinnan menetelmästä. Finanssiyhteisöjen olisi näiden toimintaperiaatteiden ja menettelyjen yhteydessä otettava käyttöön tarpeisiinsa sopivat testauskäytännöt ja -menetelmät, noudatettava riskiperusteista lähestymistapaa ja varmistettava, että ylläpidetään turvallista, luotettavaa ja joustavaa TVT-ympäristöä. TVT-hankkeen turvallisen toteutuksen takaamiseksi finanssiyhteisöjen olisi varmistettava, että henkilöstö tietyiltä liiketoiminnan osa-alueilta tai tietyistä tehtävistä, joihin kyseinen TVT-hanke vaikuttaa, voi tarjota tarvittavaa tietoa ja asiantuntemusta. Tehokkaan valvonnan varmistamiseksi ylimmälle hallintoelimelle olisi toimitettava raportit TVT-hankkeista, erityisesti hankkeista, jotka vaikuttavat kriittisiin tai tärkeisiin toimintoihin, ja niihin liittyvistä riskeistä. Finanssiyhteisöjen olisi räätälöitävä järjestelmällisten ja meneillään olevien tarkastelujen ja raporttien laatimistiheys ja yksityiskohdat niihin liittyvien TVT-hankkeiden tärkeyden ja koon mukaan.

(16) On tarpeen varmistaa, että tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen hankkimat ja kehittämät ohjelmistopaketit integroidaan tehokkaasti ja turvallisesti nykyiseen TVT-ympäristöön vakiintuneiden liiketoiminta- ja tietoturvatavoitteiden mukaisesti. Finanssiyhteisöjen olisi sen vuoksi arvioitava tällaiset ohjelmistopaketit perusteellisesti. Tätä varten sekä haavoittuvuuksien ja mahdollisten turvallisuuspuutteiden tunnistamiseksi ohjelmistopaketeissa ja laajemmissa TVT-järjestelmissä finanssiyhteisöjen olisi suoritettava TVT-turvallisuuden testaus. Jotta voidaan arvioida ohjelmiston eheyttä ja varmistaa, että ohjelmiston käyttö ei aiheuta riskejä TVT-turvallisuudelle, finanssiyhteisöjen olisi myös tarkistettava hankittujen ohjelmistojen lähdekoodit käyttäen sekä staattisia että dynaamisia testausmenetelmiä. Tämä koskee myös mahdollisuuksien mukaan TVT-palveluntarjoajana olevien kolmansien osapuolten tarjoamia omistusoikeudellisia ohjelmistoja.

(17) Muutoksiin liittyy niiden laajuudesta riippumatta luontaisia riskejä, jopa merkittäviä riskejä tietojen luottamuksellisuuden, eheyden ja saatavuuden heikkenemisestä, ja ne voivat siten johtaa vakaviin liiketoiminnan häiriöihin. Jotta finanssiyhteisöt voidaan suojata mahdollisilta TVT-haavoittuvuuksilta ja -heikkouksilta, jotka voivat altistaa ne merkittäville riskeille, tarvitaan tiukka todentamisprosessi, jolla varmistetaan, että kaikki muutokset täyttävät tarvittavat TVT-turvallisuusvaatimukset. Tämän asetuksen II osastossa tarkoitetuilla finanssiyhteisöillä olisi sen vuoksi oltava käytössään vakaat TVT-muutosten hallintaa koskevat toimintaperiaatteet ja menettelyt olennaisena osana niiden TVT-turvallisuutta koskevia toimintaperiaatteita ja menettelyjä. TVT-muutosten hallintaa koskevan prosessin objektiivisuuden ja tehokkuuden säilyttämiseksi, eturistiriitojen ehkäisemiseksi ja sen varmistamiseksi, että TVT-muutoksia arvioidaan objektiivisesti, on tarpeen erottaa toisistaan muutosten hyväksymisestä vastaavat toiminnot sekä muutoksia pyytävät ja muutokset toteuttavat toiminnot. Jotta siirtymät tapahtuvat tehokkaasti, TVT-muutokset toteutetaan hallitusti ja TVT-järjestelmien toimintaan aiheutuu mahdollisimman vähäiset häiriöt, finanssiyhteisöjen olisi osoitettava selkeät tehtävät ja vastuut, joilla varmistetaan, että TVT-muutokset toteutetaan suunnitellusti, testataan asianmukaisesti ja että niiden laatu varmistetaan. Sen varmistamiseksi, että TVT-järjestelmien tehokkaan toiminnan jatkuvuus turvataan, ja jotta finanssiyhteisöillä olisi turvaverkko, finanssiyhteisöjen olisi myös laadittava ja otettava käyttöön varamenettelyjä. Finanssiyhteisöjen olisi selkeästi määritettävä tällaiset varamenettelyt ja osoitettava vastuualueet, joilla varmistetaan nopea ja tehokas reagointi, jos TVT-muutokset epäonnistuvat.

(18) TVT:hen liittyvien poikkeamien havaitsemiseksi, hallitsemiseksi ja niistä raportoimiseksi tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi otettava käyttöön TVT:hen liittyviä poikkeamia koskevat toimintaperiaatteet, jotka kattavat TVT:hen liittyvien poikkeamien hallintaprosessin eri osatekijät. Tätä varten finanssiyhteisöjen olisi määritettävä kaikki asiaankuuluvat organisaation sisä- ja ulkopuoliset yhteyspisteet, jotka voivat helpottaa prosessin eri vaiheiden asianmukaista koordinointia ja täytäntöönpanoa. Suuntaukset TVT:hen liittyvissä poikkeamissa antavat finanssiyhteisöille arvokasta tietoa, jonka avulla ne voivat tehokkaasti tunnistaa poikkeamien juurisyyt ja perimmäiset ongelmat ja reagoida niihin. Jotta voidaan optimoida TVT:hen liittyvien poikkeamien havaitseminen ja niihin reagoiminen ja tunnistaa suuntauksia poikkeamissa, finanssiyhteisöjen olisi erityisesti analysoitava yksityiskohtaisesti TVT:hen liittyviä poikkeamia, joita ne pitävät merkittävimpinä muun muassa niiden säännöllisen toistumisen vuoksi.

(19) Poikkeavan toiminnan varhaisen ja tehokkaan havaitsemisen varmistamiseksi tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi kerättävä, seurattava ja analysoitava eri tietolähteitä ja osoitettava tähän liittyvät tehtävät ja vastuut. Sisäisten tietolähteiden osalta lokitiedot ovat erittäin tärkeä tietolähde, mutta finanssiyhteisöt eivät saisi nojata ainoastaan lokitietoihin. Sen sijaan finanssiyhteisöjen olisi tarkasteltava tietoja laajemmin siten, että otetaan huomioon muiden sisäisten toimintojen raportoimat tiedot, koska kyseiset toiminnot ovat usein arvokas merkityksellisten tietojen lähde. Samasta syystä finanssiyhteisöjen olisi analysoitava ja seurattava ulkoisista lähteistä kerättyjä tietoja, mukaan lukien TVT-palveluntarjoajana olevien kolmansien osapuolten toimittamat tiedot niiden järjestelmiin ja verkkoihin vaikuttavista poikkeamista, sekä muista tietolähteistä, joita finanssiyhteisöt pitävät merkityksellisinä, kerättyjä tietoja. Unionin tietosuojalainsäädäntöä sovelletaan tällaisiin tietoihin, jos ne sisältävät henkilötietoja. Henkilötiedot olisi rajoitettava siihen, mikä on tarpeen poikkeaman havaitsemiseksi.

(20) TVT:hen liittyvien poikkeamien havaitsemisen helpottamiseksi finanssiyhteisöjen olisi säilytettävä poikkeamia koskeva näyttö. Jotta voidaan yhtäältä varmistaa, että tällainen näyttö säilytetään riittävän pitkään, ja toisaalta välttää liiallinen sääntelytaakka, finanssiyhteisöjen olisi määritettävä säilytysaika ottaen huomioon muun muassa tietojen kriittisyys ja unionin lainsäädännöstä johtuvat säilyttämisvaatimukset.

(21) Jotta TVT:hen liittyvät poikkeamat varmasti havaitaan ajoissa, tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen ei tulisi rajoittua ainoastaan niihin kriteereihin, joiden on määritetty käynnistävän TVT:hen liittyvien poikkeamien havaitsemisen ja niihin reagoimisen. Lisäksi vaikka finanssiyhteisöjen olisi otettava huomioon kukin näistä kriteereistä, TVT:hen liittyvien poikkeamien havaitsemisen ja niihin reagoimisen käynnistämisen edellytyksenä ei tulisi olla kaikkien kriteereissä kuvattujen olosuhteiden esiintyminen samanaikaisesti. Kyseisten TVT-palvelujen merkitys olisi myös otettava asianmukaisesti huomioon.

(22) Kun tämän asetuksen II osastossa tarkoitetut finanssiyhteisöt laativat TVT-liiketoiminnan jatkuvuutta koskevia toimintaperiaatteitaan, niiden olisi otettava huomioon TVT-riskinhallinnan olennaiset osatekijät, mukaan lukien TVT:hen liittyvien poikkeamien hallintastrategiat ja poikkeamia koskevat viestintästrategiat, TVT-muutoksenhallintaprosessit sekä TVT-palveluntarjoajana oleviin kolmansiin osapuoliin liittyvät riskit.

(23) On tarpeen vahvistaa skenaariot, jotka tämän asetuksen II osastossa tarkoitettujen finanssiyhteisöjen olisi otettava huomioon niin TVT:tä koskevien reagointi- ja palautumissuunnitelmien täytäntöönpanossa kuin TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien testauksessa. Skenaarioiden olisi toimittava lähtökohtana finanssiyhteisöille, kun ne analysoivat kunkin skenaarion merkityksellisyyttä ja uskottavuutta sekä tarvetta kehittää vaihtoehtoisia skenaarioita. Finanssiyhteisöjen olisi keskityttävä skenaarioihin, joihin liittyen investoinnit häiriönsietokykyä parantaviin toimenpiteisiin olisivat tehokkaimpia ja tuloksekkaimpia. Finanssilaitosten olisi testattava vaihtoa ensisijaisen TVT-infrastruktuurin ja mahdollisen varakapasiteetin, varmuuskopioiden ja varajärjestelmien välillä ja arvioitava tämän avulla, toimivatko kyseinen varakapasiteetti ja kyseiset varmuuskopiot ja varajärjestelmät tehokkaasti riittävän ajan, ja varmistettava, että ensisijaisen TVT-infrastruktuurin normaali toiminta palautetaan palautumistavoitteiden mukaisesti.

(24) On tarpeen vahvistaa operatiivista riskiä koskevat vaatimukset ja erityisesti TVT-hankkeiden ja -muutosten hallintaa sekä TVT-liiketoiminnan jatkuvuuden hallintaa koskevat vaatimukset, jotka perustuvat keskusvastapuoliin, arvopaperikeskuksiin ja kauppapaikkoihin Euroopan parlamentin ja neuvoston asetusten (EU) N:o 648/2012 ([3]), (EU) N:o 600/2014 ([4]) ja (EU) N:o 909/2014 ([5]) mukaisesti jo sovellettaviin vaatimuksiin.

(25) Asetuksen (EU) 2022/2554 6 artiklan 5 kohdassa edellytetään, että finanssiyhteisöt tarkastelevat TVT-riskinhallintajärjestelmäänsä uudelleen ja toimittavat toimivaltaiselle viranomaiselleen kertomuksen uudelleentarkastelusta. Jotta toimivaltaiset viranomaiset voisivat käsitellä helposti kyseisten kertomusten tietoja ja jotta varmistetaan kyseisten tietojen asianmukainen välittäminen, finanssiyhteisöjen olisi toimitettava kertomukset haut mahdollistavassa sähköisessä muodossa.

(26) Asetuksen (EU) 2022/2554 16 artiklassa tarkoitetun yksinkertaistetun TVT-riskinhallintajärjestelmän soveltamisalaan kuuluvia finanssiyhteisöjä koskevissa vaatimuksissa olisi keskityttävä niihin keskeisiin alueisiin ja osatekijöihin, jotka kyseisten finanssiyhteisöjen laajuuden, riskin, koon ja monimutkaisuuden vuoksi ovat vähintään tarpeen kyseisten finanssiyhteisöjen tietojen ja palvelujen luottamuksellisuuden, eheyden, saatavuuden ja aitouden varmistamiseksi. Tässä yhteydessä kyseisillä finanssiyhteisöillä olisi oltava käytössään sisäinen hallinta- ja valvontakehys, jossa asetetaan selkeät vastuualueet ja jolla mahdollistetaan tehokas ja vakaa riskienhallintajärjestelmä. Lisäksi kyseisten finanssiyhteisöjen olisi hallinnollisen ja operatiivisen rasitteen vähentämiseksi laadittava ja dokumentoitava vain yksi toimintapolitiikka eli tietoturvapolitiikka, jossa määritellään korkean tason periaatteet ja säännöt, jotka ovat tarpeen kyseisten finanssiyhteisöjen tietojen ja palvelujen luottamuksellisuuden, eheyden, saatavuuden ja aitouden suojaamiseksi.

(27) Tämän asetuksen säännökset liittyvät TVT-riskinhallintajärjestelmään. Niissä täsmennetään finanssiyhteisöihin asetuksen (EU) 2022/2554 15 artiklan mukaisesti sovellettavia erityisiä osatekijöitä ja laaditaan yksinkertaistettu TVT-riskinhallintajärjestelmä mainitun asetuksen 16 artiklan 1 kohdassa tarkoitettuja finanssiyhteisöjä varten. Tavanomaisen ja yksinkertaistetun TVT-riskinhallintajärjestelmän välisen johdonmukaisuuden varmistamiseksi ja ottaen huomioon, että kyseisiä säännöksiä olisi sovellettava samanaikaisesti, on aiheellista sisällyttää kyseiset säännökset yhteen säädökseen.

(28) Tämä asetus perustuu teknisten sääntelystandardien luonnoksiin, jotka Euroopan pankkiviranomainen, Euroopan vakuutus- ja lisäeläkeviranomainen ja Euroopan arvopaperimarkkinaviranomainen, jäljempänä 'Euroopan valvontaviranomaiset', ovat toimittaneet komissiolle Euroopan unionin kyberturvallisuusvirastoa (ENISA) kuullen.

([3]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 648/2012, annettu 4 päivänä heinäkuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä (EUVL L 201, 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 600/2014, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä asetuksen (EU) N:o 648/2012 muuttamisesta (EUVL L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 909/2014, annettu 23 päivänä heinäkuuta 2014, arvopaperitoimituksen parantamisesta Euroopan unionissa sekä arvopaperikeskuksista ja direktiivien 98/26/EY ja 2014/65/EU sekä asetuksen (EU) N:o 236/2012 muuttamisesta (EUVL L 257, 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1093/2010 ([6]) 54 artiklassa, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1094/2010 ([7]) 54 artiklassa ja Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1095/2010 ([8]) 54 artiklassa tarkoitettu Euroopan valvontaviranomaisten yhteiskomitea on järjestänyt avoimia julkisia kuulemisia teknisten sääntelystandardien luonnoksista, joihin tämä asetus perustuu, arvioinut ehdotettujen standardien mahdollisia kustannuksia ja hyötyjä sekä pyytänyt neuvontaa asetuksen (EU) N:o 1093/2010 37 artiklan mukaisesti perustetulta pankkialan osallisryhmältä, asetuksen (EU) N:o 1094/2010 37 artiklan mukaisesti perustetuilta vakuutus- ja jälleenvakuutusalan osallisryhmältä ja lisäeläkealan osallisryhmältä sekä asetuksen (EU) N:o 1095/2010 37 artiklan mukaisesti perustetulta arvopaperimarkkina-alan osallisryhmältä.

(30) Siltä osin kuin tässä säädöksessä säädettyjen velvoitteiden noudattaminen edellyttää henkilötietojen käsittelyä, olisi sovellettava kaikilta osin Euroopan parlamentin ja neuvoston asetuksia (EU) 2016/679 ([9]) ja (EU) 2018/1725 ([10]). Esimerkiksi silloin, kun henkilötietoja kerätään poikkeaman asianmukaisen havaitsemisen varmistamiseksi, olisi noudatettava tietojen minimoinnin periaatetta. Myös Euroopan tietosuojavaltuutettua on kuultu tämän säädöksen tekstiluonnoksesta,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

I OSASTO

YLEISET PERIAATTEET

1 artikla

Yleinen riskiprofiili ja monimutkaisuus

Kun laaditaan ja toteutetaan II osastossa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä sekä III osastossa tarkoitettua yksinkertaistettua TVT-riskinhallintajärjestelmää, on otettava huomioon finanssiyhteisön koko ja yleinen riskiprofiili sekä sen palvelujen, toiminnan ja toimintojen luonne, laajuus ja monimutkaisuutta lisäävät tai vähentävät tekijät, mukaan lukien tekijät, jotka liittyvät

a) salaukseen ja salaustekniikkaan;

b) TVT-toimien turvallisuuteen;

c) verkkoturvallisuuteen;

([6]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1093/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan pankkiviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1094/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan vakuutus- ja lisäeläkeviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/79/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1095/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan arvopaperimarkkinaviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/77/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) TVT-hankkeiden ja -muutosten hallintaan;

e) vaikutuksiin, joita TVT-riskillä mahdollisesti on tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen, sekä vaikutuksiin, joita häiriöillä mahdollisesti on finanssiyhteisön toiminnan jatkuvuuteen ja käytettävyyteen.

II OSASTO

TVT-RISKINHALLINTAVÄLINEIDEN, -MENETELMIEN, -MENETTELYIDEN JA -POLITIIKKATOIMIEN YHDENMUKAISTAMINEN ASETUKSEN (EU) 2022/2554 15 ARTIKLAN MUKAISESTI

I LUKU

TVT-turvallisuutta koskevat toimintaperiaatteet, menettelyt, protokollat ja välineet

1 jakso

2 artikla

TVT-turvallisuutta koskevien toimintaperiaatteiden, menettelyjen, protokollien ja välineiden yleiset osatekijät

1. Finanssiyhteisöjen on varmistettava, että niiden TVT-turvallisuutta koskevat toimintaperiaatteet, tietoturva ja niihin liittyvät asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitetut menettelyt, protokollat ja välineet sisällytetään niiden TVT-riskinhallintajärjestelmään. Finanssiyhteisöjen on vahvistettava tässä luvussa säädetyt TVT-turvallisuutta koskevat toimintaperiaatteet, menettelyt, protokollat ja välineet siten, että

a) niillä varmistetaan verkkojen turvallisuus;

b) niihin sisältyy asianmukainen suojaus tunkeutumisia ja tiedon väärinkäyttöä vastaan;

c) niillä turvataan tietojen saatavuus, aitous, eheys ja luottamuksellisuus, myös käyttämällä salaustekniikoita;

d) niillä taataan tietojen täsmällinen ja nopea siirtäminen ilman merkittäviä häiriöitä ja tarpeettomia viivästyksiä.

2. Finanssiyhteisöjen on varmistettava 1 kohdassa tarkoitettujen TVT-turvallisuutta koskevien toimintaperiaatteiden osalta, että

a) ne ovat linjassa asetuksen (EU) 2022/2554 6 artiklan 8 kohdassa tarkoitettuun digitaalisen häiriönsietokyvyn strategiaan sisältyvien finanssiyhteisön tietoturvatavoitteiden kanssa;

b) niissä ilmoitetaan päivä, jona ylin hallintoelin on virallisesti hyväksynyt TVT-turvallisuutta koskevat toimintaperiaatteet;

c) ne sisältävät indikaattoreita ja toimenpiteitä, joilla

   i) seurataan TVT-turvallisuutta koskevien toimintaperiaatteiden, menettelyjen, protokollien ja välineiden täytäntöönpanoa;

   ii) kirjataan poikkeamat tästä täytäntöönpanosta;

   iii) varmistetaan, että finanssiyhteisön digitaalinen häiriönsietokyky on turvattu ii alakohdassa tarkoitettujen poikkeamien varalta;

d) niissä yksilöidään henkilöstön vastuut kaikilla tasoilla finanssiyhteisön TVT-turvallisuuden varmistamiseksi;

e) niissä täsmennetään seuraukset, joita aiheutuu, jos finanssiyhteisön henkilöstö ei noudata TVT-turvallisuutta koskevia toimintaperiaatteita, jos tätä koskevia määräyksiä ei ole annettu finanssiyhteisön muissa toimintaperiaatteissa;

f) niissä luetellaan asiakirja-aineisto, joka on säilytettävä;

g) niissä määritetään tehtävien eriyttämisjärjestelyt tapauksen mukaan joko kolmen puolustuslinjan mallin tai muun sisäisen riskinhallinta- ja valvontamallin mukaisesti, jotta vältetään eturistiriidat;

h) niissä otetaan huomioon johtavat käytännöt ja tarvittaessa asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määritellyt standardit;

i) niissä määritetään TVT-turvallisuutta koskevien toimintaperiaatteiden, menettelyjen, käytäntöjen ja välineiden kehittämiseen, täytäntöönpanoon ja ylläpitoon liittyvät tehtävät ja vastuut;

j) niitä tarkastellaan uudelleen asetuksen (EU) 2022/2554 6 artiklan 5 kohdan mukaisesti;

k) niissä otetaan huomioon finanssiyhteisöä koskevat olennaiset muutokset, mukaan lukien olennaiset muutokset finanssiyhteisön toiminnassa tai prosesseissa, kyberuhkaympäristössä tai sovellettavissa oikeudellisissa velvoitteissa.

2 jakso

3 artikla

TVT-riskinhallinta

Finanssiyhteisöjen on laadittava, dokumentoitava ja otettava käyttöön TVT-riskinhallinnan toimintaperiaatteet ja menettelyt, jotka sisältävät kaikki seuraavat osatekijät:

a) ilmoitus asetuksen (EU) 2022/2554 6 artiklan 8 kohdan b alakohdan mukaisesti vahvistetun TVT-riskin riskitason hyväksymisestä;

b) TVT-riskinarviointia koskeva menettely ja menetelmät, joilla määritetään

   i) haavoittuvuudet ja uhat, jotka vaikuttavat tai voivat vaikuttaa tuettuihin liiketoimintoihin sekä TVT-järjestelmiin ja TVT-omaisuuteen, jolla kyseisiä toimintoja tuetaan;

   ii) määrälliset tai laadulliset indikaattorit, joilla mitataan i alakohdassa tarkoitettujen haavoittuvuuksien ja uhkien vaikutusta ja todennäköisyyttä;

c) menettely tunnistettujen ja arvioitujen TVT-riskien hallintatoimenpiteiden määrittämiseksi, toteuttamiseksi ja dokumentoimiseksi, mukaan lukien sellaisten TVT-riskinhallintatoimenpiteiden määrittäminen, jotka ovat tarpeen TVT-riskin saattamiseksi a alakohdassa tarkoitetulle riskitasolle;

d) niiden TVT-jäännösriskien osalta, joita edelleen esiintyy c alakohdassa tarkoitettujen TVT-riskinhallintatoimenpiteiden toteuttamisen jälkeen:

   i) määräykset kyseisten TVT-jäännösriskien tunnistamisesta;

   ii) tehtävien ja vastuiden osoittaminen seuraavien osalta:

      1) sellaisten TVT-jäännösriskien hyväksyminen, jotka ylittävät a alakohdassa tarkoitetun finanssiyhteisön riskitason;

      2) tämän d alakohdan iv alakohdassa tarkoitettu uudelleentarkasteluprosessi;

   iii) luettelon laatiminen hyväksytyistä TVT-jäännösriskeistä, mukaan lukien perustelut niiden hyväksymiselle;

   iv) määräykset hyväksyttyjen TVT-jäännösriskien uudelleentarkastelusta vähintään kerran vuodessa, mukaan lukien seuraavat:

      1) TVT-jäännösriskien mahdollisten muutosten tunnistaminen;

      2) käytettävissä olevien lieventämistoimenpiteiden arviointi;

      3) arvio siitä, ovatko TVT-jäännösriskien hyväksymisen perustelut edelleen päteviä ja sovellettavissa uudelleentarkastelun ajankohtana;

e) määräykset seuraavien seurannasta:

   i) mahdolliset muutokset TVT:hen liittyvässä riski- ja kyberuhkaympäristössä;

   ii) sisäiset ja ulkoiset haavoittuvuudet ja uhat:

   iii) finanssiyhteisön TVT-riski, jotta voidaan nopeasti havaita muutokset, jotka voivat vaikuttaa finanssiyhteisön TVT-riskiprofiiliin;

f) määräykset prosessista, jolla varmistetaan, että finanssiyhteisön liiketoimintastrategiaan ja digitaalisen häiriönsietokyvyn strategiaan tehdyt muutokset otetaan huomioon.

Sovellettaessa ensimmäisen kohdan c alakohtaa kyseisessä alakohdassa tarkoitetulla menettelyllä on varmistettava

a) toteutettujen TVT-riskinhallintatoimenpiteiden tuloksellisuuden seuranta;

b) arvio siitä, onko finanssiyhteisölle vahvistetut riskitasot saavutettu;

c) arvio siitä, onko finanssiyhteisö korjannut tai parantanut tarpeen mukaan kyseisiä toimenpiteitä.

3 jakso

TVT-omaisuudenhallinta

4 artikla

TVT-omaisuudenhallintaperiaatteet

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön TVT-omaisuudenhallintaperiaatteet.

2. Edellä 1 kohdassa tarkoitetuissa TVT-omaisuudenhallintaperiaatteissa on

a) määrättävä asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti yksilöidyn ja luokitellun TVT-omaisuuden elinkaaren seurannasta ja hallinnasta;

b) määrättävä, että finanssiyhteisö pitää kirjaa kaikista seuraavista:

   i) kunkin TVT-omaisuuserän yksilöllinen tunniste;

   ii) tiedot kaikkien TVT-omaisuuserien fyysisestä tai loogisesta sijainnista;

   iii) kaikkien TVT-omaisuuserien asetuksen (EU) 2022/2254 8 artiklan 1 kohdassa tarkoitettu luokittelu;

   iv) TVT-omaisuuserien omistajien henkilöllisyys;

   v) liiketoiminnot tai palvelut, joita TVT-omaisuuserillä tuetaan;

   vi) TVT-liiketoiminnan jatkuvuutta koskevat vaatimukset, mukaan lukien palautumisaika- ja palautumispistetavoitteet;

   vii) voiko TVT-omaisuus altistua tai altistuuko se ulkoisille verkoille, internet mukaan luettuna;

   viii) TVT-omaisuuserien ja kutakin TVT-omaisuuserää käyttävien liiketoimintojen väliset yhteydet ja keskinäiset riippuvuussuhteet;

   ix) tapauksen mukaan kunkin TVT-omaisuuserän osalta TVT-palveluntarjoajana olevan kolmannen osapuolen säännöllisten, jatkettujen ja räätälöityjen tukipalvelujen päättymispäivät, joiden jälkeen kyseisillä TVT-omaisuuserillä ei ole enää niiden toimittajan tai TVT-palveluntarjoajana olevan kolmannen osapuolen tukea;

c) muiden finanssiyhteisöjen kuin mikroyritysten tapauksessa määrättävä, että kyseiset finanssiyhteisöt pitävät kirjaa tiedoista, jotka ovat tarpeen asetuksen (EU) 2022/2554 8 artiklan 7 kohdassa tarkoitetun erityisen TVT-riskinarvioinnin tekemiseksi kaikista aiemman sukupolven TVT-järjestelmistä.

5 artikla

TVT-omaisuudenhallintamenettely

1. Finanssiyhteisöjen on laadittava, dokumentoitava ja otettava käyttöön TVT-omaisuudenhallintamenettely.

2. Edellä 1 kohdassa tarkoitetussa TVT-omaisuudenhallintamenettelyssä on täsmennettävä kriteerit, joiden perusteella arvioidaan liiketoimintoja tukevan tieto-omaisuuden ja TVT-omaisuuden kriittisyyttä. Arvioinnissa on otettava huomioon

a) kyseisiin liiketoimintoihin liittyvä TVT-riski ja liiketoimintojen riippuvuus tieto-omaisuudesta tai TVT-omaisuudesta;

b) miten tällaisen tieto-omaisuuden ja TVT-omaisuuden luottamuksellisuuden, eheyden ja saatavuuden heikkeneminen vaikuttaisi finanssiyhteisöjen liiketoimintaprosesseihin ja toimintaan.

4 jakso

Salaus ja salaustekniikka

6 artikla

Salaus ja salaustekniikkaa hyödyntävä valvonta

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteitaan, menettelyjään, protokolliaan ja välineitään laadittava, dokumentoitava ja otettava käyttöön salausta ja salaustekniikkaa hyödyntävää valvontaa koskevat toimintaperiaatteet.

2. Finanssiyhteisöjen on suunniteltava 1 kohdassa tarkoitetut salausta ja salaustekniikkaa hyödyntävää valvontaa koskevat toimintaperiaatteet hyväksytyn datan luokittelun ja TVT-riskinarvioinnin tulosten perusteella. Toimintaperiaatteisiin on sisällyttävä säännöt kaikista seuraavista:

a) tietojen salaus levossa ja siirtämisen aikana;

b) tietojen salaus käsittelyn aikana tarpeen mukaan;

c) sisäisten verkkoyhteyksien ja ulkopuolisten osapuolten kanssa käytävän liikenteen salaaminen;

d) jäljempänä 7 artiklassa tarkoitettu salausavaimen hallinta niin, että vahvistetaan salausavaimien asianmukaista käyttöä, suojaamista ja elinkaarta koskevat säännöt.

Jos tietojen salaaminen käsittelyn aikana ei ole mahdollista, finanssiyhteisöjen on b alakohtaa soveltaessaan käsiteltävä tietoja erillisessä ja suojatussa ympäristössä tai toteutettava vastaavat toimenpiteet tietojen luottamuksellisuuden, eheyden, aitouden ja saatavuuden varmistamiseksi.

3. Finanssiyhteisöjen on sisällytettävä 1 kohdassa tarkoitettuihin salausta ja salaustekniikkaa hyödyntävää valvontaa koskeviin toimintaperiaatteisiin salaustekniikoiden ja käyttötapojen valintaa koskevat kriteerit ottaen huomioon johtavat käytännöt ja asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määritellyt standardit sekä asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistettu asiaankuuluvan TVT-omaisuuden luokittelu. Finanssiyhteisöjen, jotka eivät pysty noudattamaan johtavia käytäntöjä tai standardeja tai käyttämään luotettavimpia tekniikoita, on otettava käyttöön lieventämis- ja seurantatoimenpiteitä, joilla varmistetaan kyberuhkien sietokyky.

4. Finanssiyhteisöjen on sisällytettävä 1 kohdassa tarkoitettuihin salausta ja salaustekniikkaa hyödyntävää valvontaa koskeviin toimintaperiaatteisiin määräykset salausteknologian päivittämisestä tai muuttamisesta tarvittaessa salauksen ratkonnan kehityksen perusteella. Näillä päivityksillä tai muutoksilla on varmistettava, että salausteknologian kyberuhkien sietokyky säilyy, kuten 10 artiklan 2 kohdan a alakohdassa edellytetään. Finanssiyhteisöjen, jotka eivät pysty päivittämään tai muuttamaan salausteknologiaa, on otettava käyttöön lieventämis- ja seurantatoimenpiteitä, joilla varmistetaan kyberuhkien sietokyky.

5. Finanssiyhteisöjen on sisällytettävä 1 kohdassa tarkoitettuihin salausta ja salaustekniikkaa hyödyntävää valvontaa koskeviin toimintaperiaatteisiin vaatimus 3 ja 4 kohdan mukaisesti hyväksyttyjen lieventämis- ja seurantatoimenpiteiden käyttöönoton kirjaamisesta ja käyttöönoton perustelemisesta.

7 artikla

Salausavainten hallinta

1. Finanssiyhteisöjen on sisällytettävä 6 artiklan 2 kohdan d alakohdassa tarkoitettuihin salausavainten hallintaa koskeviin toimintaperiaatteisiin vaatimukset salausavainten hallinnasta niiden koko elinkaaren ajan, mukaan lukien salausavainten tuottaminen, uusiminen, tallentaminen, varmuuskopiointi, arkistointi, haku, siirto, käytöstä poistaminen, peruuttaminen ja tuhoaminen.

2. Finanssiyhteisöjen on määritettävä ja toteutettava valvontatoimenpiteitä salausavainten suojaamiseksi katoamiselta, luvattomalta käytöltä, luovuttamiselta ja muuttamiselta niiden koko elinkaaren ajan. Finanssiyhteisöjen on suunniteltava kyseiset valvontatoimenpiteet hyväksyttyjen datan luokittelun ja TVT-riskinarvioinnin tulosten perusteella.

3. Finanssiyhteisöjen on laadittava ja otettava käyttöön menetelmät salausavainten korvaamiseksi, jos avaimet katoavat, vaarantuvat tai vahingoittuvat.

4. Finanssiyhteisöjen on perustettava rekisteri vähintään kaikista kriittisiä tai tärkeitä toimintoja tukevia TVT-omaisuuseriä koskevista sertifioinneista ja sertifikaattien tallennuslaitteista ja pidettävä sitä yllä. Finanssiyhteisöjen on pidettävä kyseinen rekisteri ajan tasalla.

5. Finanssiyhteisöjen on varmistettava sertifiointien pikainen uusiminen ennen niiden voimassaolon päättymistä.

5 jakso

TVT-toimien turvallisuus

8 artikla

TVT-toimia koskevat toimintaperiaatteet ja menettelyt

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön TVT-toimia koskevat toimintaperiaatteet ja menettelyt. Toimintaperiaatteissa ja menettelyissä on täsmennettävä, miten finanssiyhteisöt käyttävät, seuraavat ja valvovat TVT-omaisuuttaan ja miten omaisuuden toiminta palautetaan, mukaan lukien TVT-toimien dokumentointi.

2. Edellä 1 kohdassa tarkoitettujen TVT-toimia koskevien toimintaperiaatteiden ja menettelyjen on sisällettävä kaikki seuraavat:

a) kuvaus TVT-omaisuudesta, mukaan lukien kaikki seuraavat:

   i) TVT-järjestelmän turvallista asentamista, huoltoa, konfigurointia ja purkamista koskevat vaatimukset;

   ii) TVT-omaisuuden käyttämän tieto-omaisuuden hallintaa koskevat vaatimukset, mukaan lukien niiden automatisoitua ja manuaalista käsittelyä koskevat vaatimukset;

   iii) aiemman sukupolven TVT-järjestelmien määrittämistä ja valvontaa koskevat vaatimukset;

b) TVT-järjestelmien valvonta ja seuranta, mukaan lukien kaikki seuraavat:

   i) TVT-järjestelmien varmuuskopiointia ja palauttamista koskevat vaatimukset;

   ii) aikataulutusvaatimukset ottaen huomioon TVT-järjestelmien keskinäiset riippuvuussuhteet;

   iii) protokollat jäljitysketjuja ja järjestelmälokitietoja varten;

   iv) vaatimukset, joilla varmistetaan, että sisäisen tarkastuksen ja muun testauksen suorittamisesta liiketoiminnalle aiheutuvat häiriöt ovat minimaalisia;

   v) vaatimukset, jotka koskevat TVT-tuotantoympäristöjen erottamista kehitys- ja testausympäristöistä sekä muista tuotannon ulkopuolisista ympäristöistä;

   vi) vaatimukset suorittaa kehittäminen ja testaus tuotantoympäristöstä erillisissä ympäristöissä;

   vii) vaatimukset suorittaa kehittäminen ja testaus tuotantoympäristöissä;

c) virheiden käsittely TVT-järjestelmien osalta, mukaan lukien kaikki seuraavat:

i) virheiden käsittelyä koskevat menettelyt ja protokollat;

ii) tuki- ja eskalaatioyhteyspisteet, mukaan lukien ulkoiset tukipisteet odottamattomia operatiivisia tai teknisiä poikkeamia varten;

iii) TVT-järjestelmän uudelleenkäynnistys-, takaisinkierto- ja palautusmenettelyt, joita käytetään TVT-järjestelmän häiriötilanteissa.

Kun sovelletaan b alakohdan v alakohtaa, ympäristöjen erottamisessa on otettava huomioon kaikki ympäristön osatekijät, mukaan lukien tilit, tiedot ja yhteydet, kuten 13 artiklan 1 kohdan a alakohdassa edellytetään.

Kun sovelletaan b alakohdan vii alakohtaa, 1 kohdassa tarkoitetuissa toimintaperiaatteissa ja menettelyissä on määrättävä, että tapaukset, joissa testaus suoritetaan tuotantoympäristössä, on selkeästi määritetty ja perusteltu, että ne ovat määräaikaisia ja että asiaankuuluva toiminto on hyväksynyt ne 16 artiklan 6 kohdan mukaisesti. Finanssiyhteisöjen on varmistettava TVT-järjestelmien ja tuotantodatan saatavuus, luottamuksellisuus, eheys ja aitous tuotantoympäristössä toteutettavien kehittämis- ja testaustoimien aikana.

9 artikla

Kapasiteetin ja suorituskyvyn hallinta

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön kapasiteetin ja suorituskyvyn hallintaa koskevat menettelyt seuraavien osalta:

a) TVT-järjestelmiensä kapasiteettivaatimusten määrittely;

b) resurssien optimointi;

c) seurantamenettelyt, joilla ylläpidetään ja parannetaan

i) datan ja TVT-järjestelmien saatavuutta;

ii) TVT-järjestelmien tehokkuutta;

iii) TVT-kapasiteettipulan ehkäisemistä.

2. Edellä 1 kohdassa tarkoitetuilla kapasiteetin ja suorituskyvyn hallintaa koskevilla menettelyillä on varmistettava, että finanssiyhteisöt toteuttavat asianmukaisia toimenpiteitä sellaisten TVT-järjestelmien erityispiirteiden huomioon ottamiseksi, joihin liittyy pitkiä tai monimutkaisia hankinta- tai hyväksyntäprosesseja tai jotka ovat resurssi-intensiivisiä.

10 artikla

Haavoittuvuuden ja korjauspäivitysten hallinta

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön haavoittuvuuden hallintaa koskevat menettelyt.

2. Edellä 1 kohdassa tarkoitetuissa haavoittuvuuden hallintaa koskevissa menettelyissä on

a) määritettävä ja päivitettävä asiaankuuluvat ja luotettavat tietoresurssit, jotta voidaan lisätä ja ylläpitää tietoisuutta haavoittuvuuksista;

b) varmistettava, että TVT-omaisuuden automatisoitu haavoittuvuuskartoitus ja automatisoidut arvioinnit suoritetaan siten, että niiden tiheys ja laajuus ovat oikeassa suhteessa TVT-omaisuuden asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistettuun luokitteluun ja yleiseen riskiprofiiliin nähden;

c) vahvistettava

i) käsittelevätkö TVT-palveluntarjoajana olevat kolmannet osapuolet finanssiyhteisölle tarjottaviin TVT-palveluihin liittyvät haavoittuvuudet;

ii) raportoivatko kyseiset palveluntarjoajat viipymättä finanssiyhteisölle vähintään kriittisistä haavoittuvuuksista sekä tilastoista ja suuntauksista;

d) seurattava seuraavien käyttöä:

i) kriittisiä tai tärkeitä toimintoja tukevien TVT-palvelujen käyttämät kolmansien osapuolten kirjastot, mukaan lukien avoimen lähdekoodin kirjastot;

ii) TVT-palvelut, jotka finanssiyhteisö itse on kehittänyt tai jotka TVT-palveluntarjoajana oleva kolmas osapuoli on räätälöinyt tai kehittänyt finanssiyhteisöä varten;

e) vahvistettava menettelyt haavoittuvuuksista ilmoittamiseksi vastuullisesti asiakkaille, vastapuolille ja suurelle yleisölle;

f) priorisoitava havaittujen haavoittuvuuksien korjaamiseksi toteutettavat korjauspäivitykset ja muut lieventävät toimenpiteet;

g) seurattava haavoittuvuuksien korjaamista ja todennettava haavoittuvuuksien korjaaminen;

h) edellytettävä, että kaikki TVT-järjestelmiin vaikuttavat havaitut haavoittuvuudet kirjataan ja niiden korjaamista seurataan.

Sovellettaessa b alakohtaa finanssiyhteisöjen on suoritettava kriittisiä tai tärkeitä toimintoja tukevan TVT-omaisuuden automatisoitu haavoittuvuuskartoitus ja automatisoidut arvioinnit vähintään viikoittain.

Sovellettaessa c alakohtaa finanssiyhteisöjen on pyydettävä, että TVT-palveluntarjoajana olevat kolmannet osapuolet tutkivat asiaankuuluvat haavoittuvuudet, määrittävät niiden juurisyyt ja toteuttavat asianmukaiset lieventämistoimet.

Sovellettaessa d alakohtaa finanssiyhteisöjen on tarvittaessa yhteistyössä TVT-palveluntarjoajana olevan kolmannen osapuolen kanssa seurattava kolmannen osapuolen kirjastojen versiota ja mahdollisia päivityksiä. Jos on kyse käyttövalmiista (kaupallisesta) TVT-omaisuudesta tai TVT-omaisuuden komponenteista, jotka on hankittu ja joita käytetään muita kuin kriittisiä tai tärkeitä toimintoja tukevia TVT-palveluita varten, finanssiyhteisöjen on mahdollisuuksien mukaan seurattava kolmansien osapuolten kirjastojen, mukaan lukien avoimen lähdekoodin kirjastot, käyttöä.

Sovellettaessa f alakohtaa finanssiyhteisöjen on otettava huomioon haavoittuvuuden kriittisyys, asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistettu luokittelu ja sen TVT-omaisuuden riskiprofiili, johon havaitut haavoittuvuudet vaikuttavat.

3. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön korjauspäivitysten hallintaa koskevat menettelyt.

4. Edellä 3 kohdassa tarkoitetuissa korjauspäivitysten hallintaa koskevissa menettelyissä on

a) mahdollisuuksien mukaan käytettävä automatisoituja välineitä ohjelmistoihin ja laitteisiin saatavilla olevien korjauspäivitysten ja muiden päivitysten tunnistamiseen ja arvioimiseen;

b) määritettävä hätätilannemenettelyt TVT-omaisuuserien korjauspäivitysten ja muiden päivitysten tekemistä varten;

c) testattava ja käytettävä 8 artiklan 2 kohdan b alakohdan v, vi ja vii alakohdassa tarkoitettuja ohjelmistojen ja laitteiden korjauspäivityksiä ja muita päivityksiä;

d) asetettava määräajat ohjelmistojen ja laitteiden korjauspäivitysten ja muiden päivitysten asentamiselle sekä eskalaatiomenettelyt sellaisia tapauksia varten, joissa näitä määräaikoja ei voida noudattaa.

11 artikla

Tietojen ja järjestelmän turvallisuus

1. Finanssiyhteisöjen on osana asetuksen (EU) 2022/2554 9 artiklan 2 kohdassa tarkoitettuja TVT-turvallisuutta koskevia toimintaperiaatteita, menettelyjä, protokollia ja välineitä laadittava, dokumentoitava ja otettava käyttöön tietojen ja järjestelmän turvallisuutta koskeva menettely.

2. Edellä 1 kohdassa tarkoitetun tietojen ja järjestelmän turvallisuutta koskevan menettelyn on sisällettävä kaikki seuraavat tietojen ja TVT-järjestelmän turvallisuuteen liittyvät elementit asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistetun luokittelun mukaisesti:

a) tämän asetuksen 21 artiklassa tarkoitetut pääsyn rajoitukset, joilla tuetaan kunkin luokan suojavaatimuksia;

b) TVT-omaisuuden turvallisen perustason konfiguraation määrittäminen siten, että minimoidaan kyseisen TVT-omaisuuden altistuminen kyberuhkille, ja toimenpiteet, joilla tarkistetaan säännöllisesti, että kyseiset perustasot ovat tosiasiallisesti käytössä;

c) sellaisten turvatoimenpiteiden määrittäminen, joilla varmistetaan, että TVT-järjestelmiin ja päätelaitteisiin asennetaan ainoastaan hyväksyttyjä ohjelmistoja;

d) haitallisten koodien vastaisten turvatoimenpiteiden määrittäminen;

e) sellaisten turvatoimenpiteiden määrittäminen, joilla varmistetaan, että finanssiyhteisön tietojen siirtämiseen ja tallentamiseen käytetään ainoastaan hyväksyttyjä tallennusvälineitä, järjestelmiä ja päätelaitteita;

f) seuraavat vaatimukset, joilla turvataan kannettavien päätelaitteiden ja yksityisten muiden kuin kannettavien päätelaitteiden käyttö:

   i) vaatimus käyttää hallintaratkaisua, jolla mahdollistetaan päätelaitteiden hallinta ja finanssiyhteisön tietojen pyyhkiminen etäyhteyden välityksellä;

   ii) vaatimus käyttää turvamekanismeja, joita henkilöstön jäsenet tai TVT-palveluntarjoajana olevat kolmannet osapuolet eivät voi luvattomasti muuttaa, poistaa tai ohittaa;

   iii) vaatimus käyttää siirrettäviä tiedontallennuslaitteita vain, jos TVT-jäännösriski pysyy finanssiyhteisön 3 artiklan ensimmäisen kohdan a alakohdassa tarkoitetun riskitason alapuolella;

g) menettely, jolla poistetaan turvallisesti finanssiyhteisön tiloissa olevat tai ulkoisesti tallennetut tiedot, joita finanssiyhteisön ei enää tarvitse kerätä tai tallentaa;

h) menettely, jolla hävitetään tai poistetaan käytöstä turvallisesti finanssiyhteisön tiloissa olevat tai ulkoisesti säilytettävät tiedontallennuslaitteet, jotka sisältävät luottamuksellisia tietoja;

i) sellaisten turvatoimenpiteiden määrittäminen ja toteuttaminen, joilla estetään tietojen häviäminen tai vuotaminen järjestelmistä ja päätelaitteista;

j) sellaisten turvatoimenpiteiden toteuttaminen, joilla varmistetaan, että etätyö ja yksityisten päätelaitteiden käyttö eivät vaaranna finanssiyhteisön TVT-turvallisuutta;

k) TVT-palveluntarjoajana olevan kolmannen osapuolen ylläpitämien TVT-omaisuuserien tai -palvelujen osalta digitaalisen häiriönsietokyvyn ylläpitämistä koskevien vaatimusten määrittäminen ja täytäntöönpano dataluokittelun ja TVT-riskinarvioinnin tulosten mukaisesti.

Kun sovelletaan b alakohtaa, kyseisessä alakohdassa tarkoitetussa turvallisessa perustason konfiguraatiossa on otettava huomioon johtavat käytännöt ja asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määritellyissä standardeissa vahvistetut asianmukaiset tekniikat.

Sovellettaessa k alakohtaa finanssiyhteisöjen on otettava huomioon seuraavat seikat:

a) myyjän suosittelemien asetusten käyttö finanssiyhteisön ylläpitämissä osissa;

b) tietoturvallisuuteen liittyvien tehtävien ja vastuiden selkeä jako finanssiyhteisön ja TVT-palveluntarjoajana olevan kolmannen osapuolen välillä noudattaen asetuksen (EU) 2022/2554 28 artiklan 1 kohdan a alakohdassa tarkoitettua periaatetta, jonka mukaan finanssiyhteisö on täysin vastuussa TVT-palveluntarjoajana olevasta kolmannesta osapuolesta, ja mainitun asetuksen 28 artiklan 2 kohdassa tarkoitettujen finanssiyhteisöjen osalta kriittisiä tärkeitä toimintoja tukevien TVT-palvelujen käyttöä koskevien finanssiyhteisön toimintaperiaatteiden mukaisesti;

c) tarve varmistaa ja ylläpitää finanssiyhteisössä käytössä olevan palvelun hallinnointiin ja turvallisuuteen liittyvää riittävää osaamista;

d) tekniset ja organisatoriset toimenpiteet TVT-palveluntarjoajana olevan kolmannen osapuolen TVT-palveluissaan käyttämään infrastruktuuriin liittyvien riskien minimoimiseksi ottaen huomioon johtavat käytännöt ja asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määritellyt standardit.

12 artikla

Lokitietojen kirjaaminen

1. Finanssiyhteisöjen on osana tunkeutumisen ja datan väärinkäytön vastaisia turvatoimia laadittava, dokumentoitava ja otettava käyttöön lokitietojen kirjaamista koskevat menettelyt, käytännöt ja välineet.

2. Edellä 1 kohdassa tarkoitettujen lokitietojen kirjaamista koskevien menettelyjen, käytäntöjen ja välineiden on sisällettävä kaikki seuraavat:

a) kirjattavien tapahtumien määrittäminen, lokitietojen säilytysaika sekä toimenpiteet lokitietojen suojaamiseksi ja käsittelemiseksi ottaen huomioon lokitietojen luomisen tarkoitus;

b) lokitietojen yksityiskohtaisuuden sovittaminen niiden käyttötarkoitukseen ja käyttötapaan, jotta 24 artiklassa tarkoitettu poikkeava toiminta voidaan havaita tehokkaasti;

c) vaatimus kirjata lokiin tapahtumat, jotka liittyvät johonkin seuraavista:

   i) jäljempänä 21 artiklassa tarkoitettu looginen ja fyysinen pääsynvalvonta ja henkilöllisyyden hallinta;

   ii) kapasiteetin hallinta;

   iii) muutosten hallinta;

   iv) TVT-toimet, mukaan lukien TVT-järjestelmätoiminta;

   v) verkkoliikennetoiminta, mukaan lukien TVT-verkon suorituskyky;

d) toimenpiteet lokitietojärjestelmien ja lokitietojen suojaamiseksi muuttamiselta, poistamiselta ja luvattomalta käytöltä levossa, siirtämisen aikana ja tarvittaessa käsittelyn aikana;

e) toimenpiteet, joilla havaitaan lokitietojärjestelmien toimintahäiriöt;

f) finanssiyhteisön kunkin TVT-järjestelmän kellojen synkronointi dokumentoidun ja luotettavan viiteaikalähteen perusteella, sanotun kuitenkaan rajoittamatta unionin tai kansallisen lainsäädännön nojalla sovellettavien sääntelyvaatimusten soveltamista.

Sovellettaessa a alakohtaa finanssiyhteisöjen on vahvistettava säilytysaika ottaen huomioon liiketoiminta- ja tietoturvatavoitteet, syy tapahtuman kirjaamiseen lokitietoihin sekä TVT-riskinarvioinnin tulokset.

6 jakso

Verkkoturvallisuus

13 artikla

Verkkoturvallisuuden hallinta

Finanssiyhteisöjen on osana suojatoimia, joilla varmistetaan verkkojen turvallisuus tunkeutumista ja tietojen väärinkäyttöä vastaan, laadittava, dokumentoitava ja otettava käyttöön verkkoturvallisuuden hallintaa koskevat toimintaperiaatteet, menettelyt, protokollat ja välineet, mukaan lukien kaikki seuraavat:

a) TVT-järjestelmien ja -verkkojen eriyttäminen ja segmentointi ottaen huomioon

   i) niiden toimintojen kriittisyyden ja merkityksen, joita kyseisillä TVT-järjestelmillä ja -verkoilla tuetaan;

   ii) asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti laaditun luokittelun;

   iii) kyseisiä TVT-järjestelmiä ja -verkkoja käyttävän TVT-omaisuuden kokonaisriskiprofiilin;

b) kaikkien finanssiyhteisön verkkoyhteyksien ja datavirtojen dokumentointi;

c) erillisen ja tarkoitukseen varatun verkon käyttö TVT-omaisuuden hallinnointia varten;

d) verkkoon pääsyn valvontatoimenpiteiden määrittäminen ja toteuttaminen, jotta estetään ja havaitaan luvattomien laitteiden tai järjestelmien tai sellaisten päätepisteiden kautta tapahtuvat yhteydet finanssiyhteisön verkkoon, jotka eivät täytä finanssiyhteisön turvallisuusvaatimuksia;

e) yritysverkkojen, julkisten verkkojen, kotimaisten verkkojen, kolmansien osapuolten verkkojen ja langattomien verkkojen kautta kulkevien verkkoyhteyksien salaaminen käytettyjä viestintäprotokollia varten ottaen huomioon hyväksytyn tietoluokittelun tulokset, TVT-riskinarvioinnin tulokset ja 6 artiklan 2 kohdassa tarkoitettu verkkoyhteyksien salaus;

f) verkkojen suunnittelu finanssiyhteisön vahvistamien TVT-turvallisuusvaatimusten mukaisesti ottaen huomioon johtavat käytännöt, joilla varmistetaan verkon luottamuksellisuus, eheys ja käytettävyys;

g) sisäisten verkkojen sekä internetin ja muiden ulkoisten yhteyksien välisen verkkoliikenteen suojaaminen;

h) tehtävien ja vastuiden sekä vaiheiden määrittäminen palomuuria koskevien sääntöjen ja yhteyssuodattimien määrittelyä, täytäntöönpanoa, hyväksymistä, muuttamista ja tarkistamista varten;

i) verkkoarkkitehtuurin ja verkon turvallisuussuunnittelun tarkastelu kerran vuodessa, tai mikroyritysten osalta säännöllisesti, mahdollisten haavoittuvuuksien tunnistamiseksi;

j) toimenpiteet, joilla aliverkot, verkon osat ja verkkolaitteet voidaan tarvittaessa tilapäisesti eristää;

k) kaikkien verkon osien turvallisen perustason konfiguraation käyttöönotto sekä verkon ja verkkolaitteiden suojaaminen myyjän ohjeiden, soveltuvin osin asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määriteltyjen standardien sekä johtavien käytäntöjen mukaisesti;

l) menettelyt, joilla rajoitetaan järjestelmä- ja etäistuntoja sekä lukitaan ja lopetetaan järjestelmä- ja etäistunnot tietyn ajanjakson jälkeen;

m) verkkopalvelusopimusten osalta:

   i) kaikkien verkkopalvelujen TVT- ja tietoturvatoimenpiteiden, palvelutasojen ja hallintaa koskevien vaatimusten yksilöinti ja määrittely;

   ii) sen määrittäminen, tarjoaako kyseiset palvelut konsernin sisäinen TVT-palveluntarjoaja vai TVT-palveluntarjoajana oleva kolmas osapuoli.

Sovellettaessa h alakohtaa finanssiyhteisöjen on tarkasteltava palomuuria koskevia sääntöjä ja yhteyssuodattimia säännöllisesti asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistetun luokittelun ja asianomaisten TVT-järjestelmien yleisen riskiprofiilin mukaisesti. Kriittisiä tai tärkeitä toimintoja tukevien TVT-järjestelmien osalta finanssiyhteisöjen on tarkistettava olemassa olevien palomuuria koskevien sääntöjen ja yhteyssuodattimien riittävyys vähintään kuuden kuukauden välein.

14 artikla

Tietojen suojaaminen siirtämisen aikana

1. Finanssiyhteisöjen on osana suojatoimia, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, laadittava, dokumentoitava ja otettava käyttöön toimintaperiaatteet, menettelyt, protokollat ja välineet tietojen suojaamiseksi siirtämisen aikana. Finanssiyhteisöjen on erityisesti varmistettava kaikki seuraavat:

a) tietojen saatavuus, aitous, eheys ja luottamuksellisuus verkossa tapahtuvan siirron aikana sekä sellaisten menettelyjen vahvistaminen, joilla voidaan arvioida kyseisten vaatimusten noudattamista;

b) tietovuotojen ehkäiseminen ja havaitseminen sekä suojattu tietojen siirto finanssiyhteisön ja ulkopuolisten osapuolten välillä;

c) finanssiyhteisön ja kolmansien osapuolten henkilöstöön sovellettavien luottamuksellisuutta tai salassapitojärjestelyjä koskevien vaatimusten käyttöönotto, dokumentointi ja säännöllinen tarkistaminen finanssiyhteisön tietojen suojaamistarpeita vastaavalla tavalla.

2. Finanssiyhteisöjen on suunniteltava 1 kohdassa tarkoitetut tietojen suojaamista siirtämisen aikana koskevat toimintaperiaatteet, menettelyt, protokollat ja välineet hyväksyttyjen datan luokittelun ja TVT-riskinarvioinnin tulosten perusteella.

7 jakso

TVT-hankkeiden ja -muutosten hallinta

15 artikla

TVT-projektinhallinta

1. Finanssiyhteisöjen on osana suojatoimia, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, laadittava, dokumentoitava ja otettava käyttöön TVT-projektinhallinnan periaatteet.

2. Edellä 1 kohdassa tarkoitetuissa TVT-projektinhallinnan periaatteissa on täsmennettävä tekijät, joilla varmistetaan finanssiyhteisön TVT-järjestelmien hankintaan, ylläpitoon ja tarvittaessa kehittämiseen liittyvien TVT-hankkeiden tehokas hallinnointi.

3. Edellä 1 kohdassa tarkoitettujen TVT-projektinhallinnan periaatteiden on sisällettävä kaikki seuraavat:

a) TVT-hankkeiden tavoitteet;

b) TVT-hankkeiden hallinnointi, mukaan lukien tehtävät ja vastuut;

c) TVT-hankkeiden suunnittelu, aikataulu ja vaiheet;

d) TVT-hankkeiden riskinarviointi;

e) asiaankuuluvat välitavoitteet;

f) muutoksenhallintavaatimukset;

g) kaikkien vaatimusten, mukaan lukien turvallisuusvaatimusten, testaaminen ja asiaankuuluva hyväksyntämenettely, kun TVT-järjestelmä otetaan käyttöön tuotantoympäristössä.

4. Edellä 1 kohdassa tarkoitetuilla TVT-projektinhallinnan periaatteilla on varmistettava TVT-hankkeen turvallinen toteutus tarjoamalla tarvittavaa tietoa ja asiantuntemusta liiketoiminta-alueelta tai toiminnoista, joihin TVT-hanke vaikuttaa.

5. Edellä 1 kohdassa tarkoitetuissa TVT-projektinhallinnan periaatteissa on 3 kohdan d alakohdassa tarkoitetun TVT-hankkeen riskinarvioinnin mukaisesti määrättävä, että finanssiyhteisön kriittisiin tai tärkeisiin toimintoihin vaikuttavien TVT-hankkeiden käynnistämisestä ja edistymisestä sekä niihin liittyvistä riskeistä raportoidaan ylimmälle hallintoelimelle

a) yksittäin tai kootusti TVT-hankkeiden tärkeydestä ja laajuudesta riippuen;

b) määräajoin ja tarvittaessa tapahtumakohtaisesti.

16 artikla

TVT-järjestelmien hankinta, kehittäminen ja ylläpito

1. Finanssiyhteisöjen on osana suojatoimia, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, laadittava, dokumentoitava ja otettava käyttöön TVT-järjestelmien hankintaa, kehittämistä ja ylläpitoa koskevat toimintaperiaatteet. Toimintaperiaatteissa on

a) määritettävä TVT-järjestelmien hankintaan, kehittämiseen ja ylläpitoon liittyvät turvallisuuskäytännöt ja menetelmät;

b) edellytettävä, että määritetään

   i) asetuksen (EU) N:o 1025/2012 2 artiklan 4 ja 5 alakohdassa määritellyt tekniset eritelmät ja tieto- ja viestintätekniikan tekniset eritelmät;

   ii) TVT-järjestelmien hankintaa, kehittämistä ja ylläpitoa koskevat vaatimukset huomioiden erityisesti TVT-turvallisuutta koskevat vaatimukset ja se, että asianomainen liiketoiminto ja TVT-omaisuuden omistaja hyväksyvät ne finanssiyhteisön sisäisten hallintojärjestelyjen mukaisesti;

c) määritettävä toimenpiteet, joilla TVT-järjestelmien tuotantoympäristössä tapahtuvan kehittämisen, ylläpidon ja käyttöönoton aikana lievennetään riskiä kyseisten TVT-järjestelmien tahattomasta muuttamisesta tai tarkoituksellisesta manipuloinnista.

2. Finanssiyhteisöjen on 8 artiklan 2 kohdan b alakohdan v, vi ja vii alakohdan mukaisesti laadittava, dokumentoitava ja otettava käyttöön TVT-järjestelmien hankintaa, kehittämistä ja ylläpitoa koskeva menettely kaikkien TVT-järjestelmien käyttöä edeltävää ja ylläpitotoimien jälkeistä testausta ja hyväksymistä varten. Testauksen tason on oltava oikeassa suhteessa kyseisten liiketoimintamenettelyjen ja TVT-omaisuuden kriittisyyteen. Testauksella on varmistettava, että uudet TVT-järjestelmät, mukaan lukien sisäisesti kehitettyjen ohjelmistojen laatu, ovat riittäviä niiden käyttötarkoitukseen nähden.

Keskusvastapuolten on ensimmäisessä alakohdassa säädettyjen vaatimusten lisäksi otettava tarvittaessa mukaan ensimmäisessä alakohdassa tarkoitettujen testien suunnitteluun ja toteuttamiseen

a) selvitysosapuolet ja asiakkaat;

b) yhteentoimivat keskusvastapuolet;

c) muut asiaan liittyvät osapuolet.

Arvopaperikeskusten on ensimmäisessä alakohdassa säädettyjen vaatimusten lisäksi tarvittaessa otettava mukaan ensimmäisessä alakohdassa tarkoitettujen testien suunnitteluun ja toteuttamiseen

a) käyttäjät;

b) keskeisten yleishyödyllisten palvelujen ja muiden keskeisten palvelujen tarjoajat;

c) muut arvopaperikeskukset;

d) muut markkinainfrastruktuurit;

e) muut laitokset, joiden kanssa arvopaperikeskukset ovat havainneet keskinäisiä riippuvuussuhteita liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissaan.

3. Edellä 2 kohdassa tarkoitettuun menettelyyn on sisällyttävä lähdekoodin tarkastus, johon sisältyy sekä staattinen että dynaaminen testaus. Testaukseen on sisällyttävä internetiin yhteydessä olevien järjestelmien ja sovellusten turvallisuustestaus 8 artiklan 2 kohdan b alakohdan v, vi ja vii alakohdan mukaisesti. Finanssiyhteisöjen on

a) tunnistettava ja analysoitava lähdekoodin haavoittuvuuksia ja poikkeavuuksia;

b) hyväksyttävä toimintasuunnitelma näiden haavoittuvuuksien ja poikkeavuuksien korjaamiseksi;

c) seurattava toimintasuunnitelman täytäntöönpanoa.

4. Edellä 2 kohdassa tarkoitettuun menettelyyn on sisällyttävä ohjelmistopakettien turvallisuustestaus viimeistään integrointivaiheessa 8 artiklan 2 kohdan b alakohdan v, vi ja vii alakohdan mukaisesti.

5. Edellä 2 kohdassa tarkoitetussa menettelyssä on määrättävä, että

a) tuotannon ulkopuolisissa ympäristöissä säilytetään ainoastaan anonymisoituja, pseudonymisoituja tai satunnaistettuja tuotantotietoja;

b) finanssiyhteisöt suojelevat tietojen eheyttä ja luottamuksellisuutta tuotannon ulkopuolisissa ympäristöissä.

6. Poiketen siitä, mitä 5 kohdassa säädetään, 2 kohdassa tarkoitetussa menettelyssä voidaan määrätä, että tuotantotietoja säilytetään vain tiettyjä testaustilanteita varten, rajoitetun ajan ja vain jos asianomainen toiminto on hyväksynyt asian ja siitä on raportoitu TVT-riskinhallinnasta vastaavalle toiminnolle.

7. Edellä 2 kohdassa tarkoitettuun menettelyyn on sisällyttävä valvontatoimet, joilla suojataan sisäisesti kehitettyjen tai TVT-palveluntarjoajana olevan kolmannen osapuolen kehittämien ja finanssiyhteisölle toimittamien TVT-järjestelmien lähdekoodin eheys.

8. Edellä 2 kohdassa tarkoitetussa menettelyssä on määrättävä, että omistusoikeudelliset ohjelmistot ja mahdollisuuksien mukaan TVT-palveluntarjoajana olevien kolmansien osapuolten tai avoimen lähdekoodin hankkeista peräisin olevat lähdekoodit analysoidaan ja testataan 3 kohdan mukaisesti ennen niiden käyttöönottoa tuotantoympäristössä.

9. Tämän artiklan 1–8 kohtaa sovelletaan myös TVT-järjestelmiin, joita kehittävät tai hallinnoivat TVT-toiminnon ulkopuoliset käyttäjät, riskiperusteista lähestymistapaa noudattaen.

17 artikla

TVT-muutosten hallinta

1. Ohjelmistoihin, laitteistoihin, laiteohjelmistokomponentteihin, järjestelmiin tai turvallisuusparametreihin tehtävien muutosten osalta finanssiyhteisöjen on osana suojatoimia, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, sisällytettävä asetuksen (EU) 2022/2554 9 artiklan 4 kohdan e alakohdassa tarkoitettuihin TVT-muutosten hallintaa koskeviin menettelyihin kaikki seuraavat osatekijät:

a) TVT-turvallisuutta koskevien vaatimusten täyttymisen todentaminen;

b) mekanismit, joilla varmistetaan muutoksia hyväksyvien toimintojen ja muutosten pyytämisestä ja toteuttamisesta vastaavien toimintojen riippumattomuus;

c) selkeä kuvaus tehtävistä ja vastuista, jotta varmistetaan, että

   i) muutokset yksilöidään ja suunnitellaan;

   ii) siirtymä suunnitellaan asianmukaisesti;

   iii) muutokset testataan ja viimeistellään hallitusti;

   iv) käytössä on tehokas laadunvarmistus;

d) muutosten dokumentointi ja niistä ilmoittaminen, mukaan lukien seuraavat:

   i) muutoksen tarkoitus ja laajuus:

   ii) muutoksen toteuttamisaikataulu;

   iii) odotetut tulokset;

e) varamenettelyjen ja niihin liittyvien vastuiden määrittäminen, mukaan lukien menettelyt ja vastuut, jotka koskevat muutosten keskeyttämistä ja epäonnistuneista muutoksista palautumista;

f) hätämuutosten hallintaan menettelyt, protokollat ja välineet, joihin sisältyy riittävät suojatoimet;

g) menettelyt, joilla dokumentoidaan, arvioidaan ja hyväksytään hätämuutokset, mukaan lukien väliaikaiset ratkaisut ja korjauspäivitykset, niiden käyttöön ottamisen jälkeen;

h) muutoksesta nykyisiin TVT-turvallisuutta koskeviin toimenpiteisiin mahdollisesti aiheutuvien vaikutusten tunnistaminen ja sen arviointi, edellyttääkö tällainen muutos uusien TVT-turvallisuutta koskevien toimenpiteiden hyväksymistä.

2. Keskusvastapuolten ja arvopaperikeskusten on tehtävä TVT-järjestelmilleen tiukat testit simuloimalla stressiolosuhteita sen jälkeen, kun ne ovat tehneet merkittäviä muutoksia TVT-järjestelmiinsä.

Keskusvastapuolten on otettava tarvittaessa mukaan ensimmäisessä alakohdassa tarkoitettujen testien suunnitteluun ja toteuttamiseen

a) selvitysosapuolet ja asiakkaat;

b) yhteentoimivat keskusvastapuolet;

c) muut asiaan liittyvät osapuolet.

Arvopaperikeskusten on otettava tarvittaessa mukaan ensimmäisessä alakohdassa tarkoitettujen testien suunnitteluun ja toteuttamiseen

a) käyttäjät;

b) keskeisten yleishyödyllisten palvelujen ja muiden keskeisten palvelujen tarjoajat;

c) muut arvopaperikeskukset;

d) muut markkinainfrastruktuurit;

e) muut laitokset, joiden kanssa arvopaperikeskukset ovat havainneet keskinäisiä riippuvuussuhteita TVT-liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissaan.

8 jakso

18 artikla

Fyysinen turvallisuus ja ympäristön turvallisuus

1. Finanssiyhteisöjen on osana suojatoimia, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, määritettävä, dokumentoitava ja otettava käyttöön fyysisen turvallisuuden ja ympäristön turvallisuuden toimintaperiaatteet. Finanssiyhteisöjen on suunniteltava kyseiset toimintaperiaatteet kyberuhkaympäristön perusteella, asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistetun luokittelun mukaisesti ja ottaen huomioon TVT-omaisuuden ja pääsyn kohteena olevan tieto-omaisuuden yleinen riskiprofiili.

2. Edellä 1 kohdassa tarkoitettujen fyysisen turvallisuuden ja ympäristön turvallisuuden toimintaperiaatteiden on sisällettävä kaikki seuraavat:

a) viittaus 21 artiklan ensimmäisen kohdan g alakohdassa tarkoitettujen käyttöoikeuksien valvontaa koskevien toimintaperiaatteiden osaan;

b) toimenpiteet, joilla finanssiyhteisön tiloja, datakeskuksia ja finanssiyhteisön määrittämiä arkaluonteisia alueita, joissa TVT-omaisuus ja tieto-omaisuus sijaitsevat, suojataan hyökkäyksiltä, onnettomuuksilta sekä ympäristöuhkilta ja -vaaroilta;

c) toimenpiteet, joilla turvataan TVT-omaisuus sekä finanssiyhteisön tiloissa että niiden ulkopuolella ottaen huomioon asianomaiseen TVT-omaisuuteen liittyvän TVT-riskinarvioinnin tulokset;

d) toimenpiteet, joilla varmistetaan finanssiyhteisön TVT-omaisuuden, tieto-omaisuuden ja fyysisten pääsynvalvonta-laitteiden käytettävyys, aitous, eheys ja luottamuksellisuus asianmukaisen ylläpidon avulla;

e) toimenpiteet, joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus, mukaan lukien

   i) puhtaan työpöydän käytäntö papereille;

   ii) puhtaan näytön käytäntö tietojenkäsittelylaitteille.

Sovellettaessa b alakohtaa ympäristöuhkilta ja -vaaroilta suojautumistoimenpiteiden on oltava oikeassa suhteessa tilojen, datakeskusten ja nimettyjen arkaluonteisten alueiden merkitykseen sekä niissä sijaitsevien toimintojen tai TVT-järjestelmien kriittisyyteen.

Kun sovelletaan c alakohtaa, 1 kohdassa tarkoitettuihin fyysisen turvallisuuden ja ympäristön turvallisuuden toimintaperiaatteisiin on sisällyttävä toimenpiteitä, joilla suojataan valvomaton TVT-omaisuus asianmukaisesti.

II LUKU

Henkilöstöpolitiikka ja pääsynvalvonta

19 artikla

Henkilöstöpolitiikka

Finanssiyhteisöjen on sisällytettävä henkilöstöpolitiikkaansa tai muihin asiaankuuluviin toimintapolitiikkoihinsa kaikki seuraavat TVT-turvallisuuteen liittyvät seikat:

a) TVT-turvallisuuteen liittyvien erityisten vastuiden määrittäminen ja osoittaminen;

b) finanssiyhteisön TVT-omaisuutta käyttävän tai siihen pääsyoikeudet omaavan finanssiyhteisön ja TVT-palveluntarjoajana olevien kolmansien osapuolten henkilöstöä koskevat vaatimukset

i) olla tietoisia finanssiyhteisön TVT-turvallisuutta koskevista toimintaperiaatteista, menettelyistä ja protokollista ja noudattaa niitä;

ii) olla tietoisia ilmoituskanavista, jotka finanssiyhteisö on ottanut käyttöön poikkeavan käyttäytymisen havaitsemista varten, mukaan lukien soveltuvin osin Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/1937 ([11]) mukaisesti perustetut ilmoituskanavat;

iii) palauttaa finanssiyhteisölle työsuhteen päättyessä kaikki heidän hallussaan oleva, finanssiyhteisölle kuuluva TVT-omaisuus ja aineellinen tieto-omaisuus.

20 artikla

Henkilöllisyyden hallinta

1. Käyttöoikeuksien myöntämiseksi 21 artiklan mukaisesti finanssiyhteisöjen on osana pääsynhallintaoikeuksien valvontaa laadittava, dokumentoitava ja otettava käyttöön henkilöllisyyden hallintaa koskevat toimintaperiaatteet ja menettelyt, joilla varmistetaan sellaisten luonnollisten henkilöiden ja järjestelmien yksilöllinen tunnistaminen ja todentaminen, joilla on pääsy finanssiyhteisöjen tietoihin.

2. Edellä 1 kohdassa tarkoitettujen henkilöllisyyden hallintaa koskevien toimintaperiaatteiden ja menettelyjen on sisällettävä kaikki seuraavat:

a) kaikille finanssiyhteisön henkilöstön jäsenille taikka TVT-palveluntarjoajana olevien kolmansien osapuolten henkilöstölle, jo(i)lla on pääsy finanssiyhteisön tieto-omaisuuteen ja TVT-omaisuuteen, on annettava yksilöllistä käyttäjätiliä vastaava yksilöllinen henkilöllisyys, sanotun kuitenkaan rajoittamatta 21 artiklan ensimmäisen kohdan c alakohdan soveltamista;

b) elinkaarenhallintamenettely henkilöllisyyksille ja tileille, joilla hallinnoidaan kaikkien tilien luomista, muuttamista, tarkistamista ja päivittämistä, väliaikaista käytöstäpoistamista ja sulkemista.

Sovellettaessa a alakohtaa finanssiyhteisöjen on pidettävä kirjaa kaikista luoduista henkilöllisyyksistä. Nämä tiedot on säilytettävä finanssiyhteisön uudelleenjärjestelyn tai sopimussuhteen päättymisen jälkeen, sanotun kuitenkaan rajoittamatta sovellettavassa unionin ja kansallisessa lainsäädännössä säädettyjen säilyttämisvaatimusten soveltamista.

Sovellettaessa b alakohtaa finanssiyhteisöjen on mahdollisuuksien mukaan ja tarvittaessa otettava käyttöön automatisoituja ratkaisuja henkilöllisyyksien elinkaarenhallintamenettelyä varten.

21 artikla

Pääsynvalvonta

Finanssiyhteisöjen on osana pääsynhallintaoikeuksien valvontaa laadittava, dokumentoitava ja otettava käyttöön toimintaperiaatteet, jotka sisältävät kaikki seuraavat:

a) käyttöoikeuksien myöntäminen TVT-omaisuuteen tiedonsaantitarpeen, käyttötarpeen ja vähäisimpien oikeuksien periaatteiden mukaisesti, mukaan lukien etäkäyttöoikeudet ja hätätilanteen käyttöoikeudet;

b) tehtävien eriyttäminen, jonka tarkoituksena on estää perusteeton pääsy kriittisiin tietoihin tai estää sellaisten käyttöoikeuksien yhdistelmien myöntäminen, joita voidaan käyttää valvonnan kiertämiseen;

c) käyttäjien vastuuvelvollisuutta koskeva määräys, jossa rajoitetaan mahdollisuuksien mukaan yleisten ja yhteiskäyttöisten käyttäjätilien käyttöä ja varmistetaan, että käyttäjät voidaan aina tunnistaa TVT-järjestelmissä tapahtuvan toiminnan osalta;

([11]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1937, annettu 23 päivänä lokakuuta 2019, unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta (EUVL L 305, 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) TVT-omaisuuteen pääsyn rajoittamista koskeva määräys, jossa vahvistetaan valvontatoimet ja välineet luvattoman käytön estämiseksi;

e) tilinhallintamenettelyt käyttäjätilien ja yleisten tilien, mukaan lukien yleisten pääkäyttäjätilien, käyttöoikeuksien myöntämiseksi, muuttamiseksi tai peruuttamiseksi, mukaan lukien määräykset kaikista seuraavista:

   i) käyttöoikeuksien myöntämistä, tarkistamista ja peruuttamista koskevien tehtävien ja vastuiden osoittaminen;

   ii) erityis-, hätätilanne- ja järjestelmävastaavan oikeuksien myöntäminen kaikkiin TVT-järjestelmiin käyttötarpeen perusteella tai tapauskohtaisesti;

   iii) käyttöoikeuksien peruuttaminen ilman aiheetonta viivytystä työsuhteen päättyessä tai silloin, kun käyttöoikeudet eivät ole enää tarpeen;

   iv) käyttöoikeuksien päivittäminen, kun muutokset ovat tarpeen, ja vähintään kerran vuodessa kaikkien muiden kuin kriittisiä tai tärkeitä toimintoja koskevien TVT-järjestelmien osalta ja vähintään kuuden kuukauden välein kriittisiä tai tärkeitä toimintoja tukevien TVT-järjestelmien osalta;

f) todentamismenetelmät, mukaan lukien kaikki seuraavat:

   i) sellaisten todentamismenetelmien käyttö, jotka ovat oikeassa suhteessa asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistettuun luokitteluun ja TVT-omaisuuden yleiseen riskiprofiiliin ja ottaen huomioon johtavat käytännöt;

   ii) sellaisten vahvojen tunnistusmenetelmien käyttö, johtavien käytäntöjen ja tekniikoiden mukaisesti, jotka koskevat pääsyä finanssiyhteisön verkkoon etäyhteydellä, erityisoikeutettua pääsyä, pääsyä kriittisiä tai tärkeitä toimintoja tukevaan TVT-omaisuuteen tai julkisesti saatavilla olevan TVT-omaisuuden käyttöoikeutta;

g) fyysiset pääsynvalvontatoimenpiteet, mukaan lukien seuraavat:

   i) sellaisten luonnollisten henkilöiden tunnistaminen ja kirjaaminen, joilla on lupa päästä tiloihin, datakeskuksiin ja finanssiyhteisön nimeämille arkaluonteisille alueille, joissa TVT- ja tieto-omaisuus sijaitsee;

   ii) fyysisten käyttöoikeuksien myöntäminen kriittiseen TVT-omaisuuteen ainoastaan valtuutetuille henkilöille tiedonsaantitarpeen ja vähäisimpien oikeuksien periaatteiden mukaisesti ja tapauskohtaisesti;

   iii) fyysinen pääsynvalvonta tiloissa, datakeskuksissa ja finanssiyhteisön nimeämillä arkaluonteisilla alueilla, joissa TVT- ja tieto-omaisuus sijaitsee;

   iv) fyysisten käyttöoikeuksien tarkistaminen sen varmistamiseksi, että tarpeettomat käyttöoikeudet peruutetaan viipymättä.

Sovellettaessa e alakohdan i alakohtaa finanssiyhteisöjen on vahvistettava säilytysaika ottaen huomioon liiketoiminta- ja tietoturvatavoitteet, syy tapahtuman kirjaamiseen lokitietoihin sekä TVT-riskinarvioinnin tulokset.

Sovellettaessa e alakohdan ii alakohtaa finanssiyhteisöjen on mahdollisuuksien mukaan käytettävä tarkoitukseen varattuja tilejä TVT-järjestelmiä koskevien hallinnollisten tehtävien suorittamiseen. Finanssiyhteisöjen on mahdollisuuksien mukaan ja tarvittaessa otettava käyttöön automatisoituja ratkaisuja erityisoikeuksien hallintaa varten.

Sovellettaessa g alakohdan i alakohtaa määrittämisen ja kirjaamisen on oltava oikeassa suhteessa tilojen, datakeskusten ja nimettyjen arkaluonteisten alueiden merkitykseen sekä niissä sijaitsevien toimintojen tai TVT-järjestelmien kriittisyyteen.

Sovellettaessa g alakohdan iii alakohtaa valvonnan on oltava oikeassa suhteessa asetuksen (EU) 2022/2554 8 artiklan 1 kohdan mukaisesti vahvistettuun luokitteluun ja pääsyn kohteena olevan alueen kriittisyyteen.

III LUKU

TVT:hen liittyvien poikkeamien havaitseminen ja niihin reagointi

22 artikla

TVT:hen liittyvien poikkeamien hallinnan toimintaperiaatteet

Finanssiyhteisöjen on osana mekanismeja, joilla havaitaan poikkeavaa toimintaa, mukaan lukien TVT-verkon suorituskykyyn liittyvät ongelmat ja TVT:hen liittyvät poikkeamat, laadittava, dokumentoitava ja otettava käyttöön TVT:hen liittyviä poikkeamia koskevat toimintaperiaatteet, joiden avulla niiden on

a) dokumentoitava asetuksen (EU) 2022/2554 17 artiklassa tarkoitettu TVT:hen liittyvien poikkeamien hallintaprosessi;

b) laadittava luettelo sisäisissä toiminnoissa ja ulkoisissa sidosryhmissä olevista yhteyspisteistä, jotka osallistuvat suoraan TVT-toimien turvallisuuteen, mukaan lukien

   i) kyberuhkien havaitsemiseen ja seurantaan;

   ii) poikkeavan toiminnan havaitsemiseen;

   iii) haavoittuvuuksien hallintaan;

c) laadittava, toteutettava ja käytettävä teknisiä, organisatorisia ja operatiivisia mekanismeja, joilla tuetaan TVT:hen liittyvien poikkeamien hallintaprosessia, mukaan lukien mekanismit, joiden avulla voidaan nopeasti havaita poikkeava toiminta ja käyttäytyminen tämän asetuksen 23 artiklan mukaisesti;

d) säilytettävä komission delegoidun asetuksen (EU) 2024/1772 ([12]) 15 artiklan ja unionin oikeuden nojalla mahdollisesti sovellettavien säilyttämisvaatimusten mukaisesti kaikki TVT:hen liittyviin poikkeamiin liittyvä näyttö tietyn ajan, joka ei saa olla pidempi kuin on tarpeen niihin tarkoituksiin, joita varten tiedot on kerätty, ja joka on oikeassa suhteessa asianomaisten liiketoimintojen, tukiprosessien sekä TVT- ja tieto-omaisuuden kriittisyyteen;

e) laadittava ja otettava käyttöön mekanismit, joilla analysoidaan merkittäviä tai toistuvia TVT:hen liittyviä poikkeamia ja TVT:hen liittyvien poikkeamien lukumäärässä ja esiintymistiheydessä esiintyviä kaavoja.

Sovellettaessa d alakohtaa finanssiyhteisöjen on säilytettävä kyseisessä alakohdassa tarkoitettu näyttö tietoturvallisesti.

23 artikla

Poikkeavan toiminnan havaitseminen ja kriteerit TVT:hen liittyvien poikkeamien havaitsemiseen ja niihin reagointiin

1. Finanssiyhteisöjen on vahvistettava selkeät tehtävät ja vastuut, jotta TVT:hen liittyvät poikkeamat ja poikkeava toiminta voidaan havaita ja niihin voidaan reagoida tehokkaasti.

2. Asetuksen (EU) 2022/2554 10 artiklan 1 kohdassa tarkoitetulla mekanismilla, jolla voidaan nopeasti havaita poikkeava toiminta, mukaan lukien TVT-verkon suorituskykyyn liittyvät ongelmat ja TVT:hen liittyvät poikkeamat, finanssiyhteisöjen on voitava

a) kerätä, seurata ja analysoida kaikkia seuraavia:

   i) sisäiset ja ulkoiset tekijät, mukaan lukien vähintään tämän asetuksen 12 artiklan mukaisesti kerätyt lokitiedot, liiketoiminnoista ja TVT-toiminnoista saadut tiedot sekä finanssiyhteisön käyttäjien ilmoittamat ongelmat;

   ii) mahdolliset sisäiset ja ulkoiset kyberuhat ottaen huomioon uhkatoimijoiden yleisesti käyttämät skenaariot ja uhkatiedusteluun perustuvat skenaariot;

([12]) Komission delegoitu asetus (EU) 2024/1772, annettu 13 päivänä maaliskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 täydentämisestä teknisillä sääntelystandardeilla, joissa täsmennetään TVT:hen liittyvien poikkeamien ja kyberuhkien luokittelukriteerit, vahvistetaan olennaisuusrajat ja täsmennetään laajavaikutteisia poikkeamia koskevien raporttien yksityiskohdat (EUVL L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) finanssiyhteisön TVT-palveluntarjoajana olevan kolmannen osapuolen tekemä ilmoitus TVT:hen liittyvästä poikkeamasta, joka on havaittu TVT-palveluntarjoajana olevan kolmannen osapuolen TVT-järjestelmissä ja -verkoissa ja joka voi vaikuttaa finanssiyhteisöön;

b) tunnistaa poikkeava toiminta ja käyttäytyminen ja ottaa käyttöön välineitä, joilla tehdään hälytyksiä poikkeavasta toiminnasta ja käyttäytymisestä, ainakin kriittisiä tai tärkeitä toimintoja tukevan TVT- ja tieto-omaisuuden osalta;

c) priorisoitava b alakohdassa tarkoitetut hälytykset, jotta havaittuja TVT:hen liittyviä poikkeamia voidaan hallita finanssiyhteisöjen määrittämässä odotetussa ratkaisuajassa sekä työaikana että työajan ulkopuolella;

d) kirjata, analysoida ja arvioida automaattisesti tai manuaalisesti asiaankuuluvat tiedot kaikesta poikkeavasta toiminnasta ja käyttäytymisestä.

Kun sovelletaan b alakohtaa, kyseisessä alakohdassa tarkoitettuihin välineisiin on sisällyttävä välineet, jotka tekevät automaattisia hälytyksiä ennalta määritettyjen sääntöjen perusteella sellaisten poikkeamien tunnistamiseksi, jotka vaikuttavat tietolähteiden taikka lokitietojen keruun täydellisuuteen ja eheyteen.

3. Finanssiyhteisöjen on suojattava poikkeavan toiminnan osoittava näyttö muuttamiselta ja luvattomalta pääsyltä levossa, siirtämisen aikana ja tarvittaessa käsittelyn aikana.

4. Finanssiyhteisöjen on kirjattava kaikki merkitykselliset tiedot kaikesta havaitusta poikkeavasta toiminnasta, jotta voidaan

a) yksilöidä poikkeavan toiminnan tapahtumapäivä ja -aika;

b) yksilöidä poikkeavan toiminnan havaitsemispäivä ja -aika;

c) yksilöidä poikkeavan toiminnan tyyppi.

5. Finanssiyhteisöjen on otettava huomioon kaikki seuraavat kriteerit, joiden perusteella käynnistetään asetuksen (EU) 2022/2554 10 artiklan 2 kohdassa tarkoitetut menettelyt TVT:hen liittyvien poikkeamien havaitsemiseksi ja niihin reagoimiseksi:

a) tiedot siitä, että TVT-järjestelmässä tai -verkossa on saatettu harjoittaa haitallista toimintaa tai että tällainen TVT-järjestelmä tai -verkko on saattanut vaarantua;

b) tietojen heikentynyt saatavuus, aitous, eheys ja luottamuksellisuus;

c) finanssiyhteisön liiketoimissa ja toiminnoissa havaittu haittavaikutus;

d) TVT-järjestelmien ja -verkon toiminnan keskeytyminen.

6. Sovellettaessa 5 kohtaa finanssiyhteisöjen on otettava huomioon myös vaikutusten kohteena olevien palvelujen kriittisyys.

IV LUKU

TVT-liiketoiminnan jatkuvuuden hallinta

24 artikla

TVT-liiketoiminnan jatkuvuutta koskevien toimintaperiaatteiden osatekijät

1. Finanssiyhteisöjen on sisällytettävä asetuksen (EU) 2022/2554 11 artiklan 1 kohdassa tarkoitettuihin TVT-liiketoiminnan jatkuvuutta koskeviin toimintaperiaatteisiinsa kaikki seuraavat:

a) kuvaus seuraavista:

i) TVT-liiketoiminnan jatkuvuutta koskevien toimintaperiaatteiden tavoitteet, mukaan lukien TVT- ja yleisen liiketoiminnan jatkuvuuden välinen suhde, ottaen huomioon asetuksen (EU) 2022/2554 11 artiklan 5 kohdassa tarkoitetun liiketoiminnan vaikutusanalyysin tulokset;

ii) TVT-liiketoiminnan jatkuvuutta koskevien järjestelyjen, suunnitelmien, menettelyjen ja mekanismien soveltamisala, mukaan lukien rajoitukset ja poissulkemiset;

iii) TVT-liiketoiminnan jatkuvuutta koskevien järjestelyjen, suunnitelmien, menettelyjen ja mekanismien kattama aikataulu;

iv) kriteerit TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien, TVT-reagointi- ja palautumissuunnitelmien sekä kriisiviestintäsuunnitelmien aktivoimiseksi ja deaktivoimiseksi;

b) määräykset seuraavista:

i) TVT-liiketoiminnan jatkuvuutta koskevien toimintaperiaatteiden täytäntöönpanosta vastaava hallinto ja organisaatio, mukaan lukien tehtävät, vastuut ja eskalaatiomenettelyt, joilla varmistetaan, että käytössä on riittävät resurssit;

ii) TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien ja yleistä liiketoiminnan jatkuvuutta koskevien suunnitelmien yhdenmukaistaminen vähintään kaikkien seuraavien osalta:

1) mahdolliset vikaskenaariot, mukaan lukien tämän asetuksen 26 artiklan 2 kohdassa tarkoitetut skenaariot;

2) palautumistavoitteet, joissa täsmennetään, että finanssiyhteisön on pystyttävä palauttamaan kriittiset ja tärkeät toiminnot häiriöiden jälkeen palautumisaika- ja palautumispistetavoitteen mukaisesti;

iii) TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien laatiminen vakavia liiketoiminnan häiriöitä varten osana näitä suunnitelmia ja TVT-liiketoiminnan jatkuvuutta koskevien toimien priorisointi riskiperusteista lähestymistapaa käyttäen;

iv) TVT-reagointi- ja palautumissuunnitelmien kehittäminen, testaaminen ja tarkistaminen tämän asetuksen 25 ja 26 artiklan mukaisesti;

v) käyttöön otettujen TVT-liiketoiminnan jatkuvuutta koskevien järjestelyjen, suunnitelmien, menettelyjen ja mekanismien tehokkuuden tarkastelu tämän asetuksen 26 artiklan mukaisesti;

vi) TVT-liiketoiminnan jatkuvuutta koskevien toimintaperiaatteiden linjaaminen

1) asetuksen (EU) 2022/2554 14 artiklan 2 kohdassa tarkoitetun viestintäpolitiikan kanssa;

2) asetuksen (EU) 2022/2554 11 artiklan 2 kohdan e alakohdassa tarkoitettujen viestintä- ja kriisinhallintatoimien kanssa.

2. Edellä 1 kohdassa tarkoitettujen vaatimusten lisäksi keskusvastapuolten on varmistettava, että niiden TVT-liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissa

a) on niiden kriittisten toimintojen palautumiselle enimmäisaika, joka on enintään kaksi tuntia;

b) otetaan huomioon ulkoiset sidokset ja keskinäiset riippuvuussuhteet finanssi-infrastruktuureissa, mukaan lukien keskusvastapuolen määrittämät kauppapaikat, arvopapereiden selvitys- ja maksujärjestelmät sekä keskusvastapuolen tai siihen yhteydessä olevan keskusvastapuolen käyttämät luottolaitokset;

c) edellytetään, että käytössä on järjestelyt, joilla

i) varmistetaan keskusvastapuolen kriittisten tai tärkeiden toimintojen jatkuvuus katastrofiskenaarioiden perusteella;

ii) pidetään yllä toissijaista käsittelypaikkaa, jolla voidaan varmistaa keskusvastapuolen kriittisten tai tärkeiden toimintojen jatkuvuus samalla tavalla kuin ensisijaisessa paikassa;

iii) pidetään yllä toissijaista liiketoimipaikkaa tai saadaan välittömästi pääsy toissijaiseen liiketoimipaikkaan, jotta henkilöstö voi varmistaa palvelun jatkuvuuden, jos ensisijainen liiketoimintapaikka ei ole käytettävissä;

iv) otetaan huomioon ylimääräisten käsittelypaikkojen tarve erityisesti, jos ensisijainen ja toissijainen paikka eivät ole riskiprofiileiltaan riittävän erilaisia varmistamaan sen, että keskusvastapuolen liiketoiminnan jatkuvuutta koskevat tavoitteet saavutetaan kaikissa skenaarioissa.

Sovellettaessa a alakohtaa keskusvastapuolten on kaikissa olosuhteissa saatettava päätökseen pankkipäivän lopetukseen liittyvät menettelyt ja maksut vaadittuna aikana ja päivänä.

Sovellettaessa c alakohdan i alakohtaa kyseisessä alakohdassa tarkoitetuissa järjestelyissä on käsiteltävä riittävien henkilöresurssien saatavuutta, kriittisten toimintojen seisokkiajan enimmäispituutta, automaattista vaihtoa varajärjestelmään sekä palautumista toissijaisessa käsittelypaikassa.

Sovellettaessa c alakohdan ii alakohtaa kyseisessä alakohdassa tarkoitetun toissijaisen käsittelypaikan maantieteellisen riskiprofiilin on oltava erilainen kuin ensisijaisen käsittelypaikan.

3. Edellä 1 kohdassa tarkoitettujen vaatimusten lisäksi arvopaperikeskusten on varmistettava, että niiden TVT-liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissa

a) otetaan huomioon mahdolliset yhteydet ja keskinäiset riippuvuussuhteet käyttäjiin, keskeisten yleishyödyllisten palvelujen ja keskeisten palvelujen tarjoajiin, muihin arvopaperikeskuksiin ja muihin markkinainfrastruktuureihin;

b) edellytetään, että niiden TVT-liiketoiminnan jatkuvuutta koskevissa järjestelyissä varmistetaan, että niiden kriittisten tai tärkeiden toimintojen palautumisaikatavoite ei ylitä kahta tuntia.

4. Edellä 1 kohdassa tarkoitettujen vaatimusten lisäksi kauppapaikkojen on varmistettava, että niiden TVT-liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissa varmistetaan, että

a) kaupankäynti voidaan aloittaa uudelleen kahden tunnin kuluessa tai lähes kahden tunnin kuluessa häiriöstä;

b) häiriön jälkeen mistä tahansa kauppapaikan tietoteknisestä palvelusta mahdollisesti menetettävien tietojen enimmäismäärä on lähellä nollaa.

25 artikla

TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien testaus

1. Kun finanssiyhteisöt testaavat TVT-liiketoiminnan jatkuvuutta koskevia suunnitelmia asetuksen (EU) 2022/2554 11 artiklan 6 kohdan mukaisesti, niiden on otettava huomioon tämän asetuksen 3 artiklan 1 kohdan b alakohdassa tarkoitettu finanssiyhteisön liiketoiminnan vaikutusanalyysi ja TVT-riskinarviointi.

2. Finanssiyhteisöjen on arvioitava testaamalla 1 kohdassa tarkoitettuja TVT-liiketoiminnan jatkuvuutta koskevia suunnitelmiaan, pystyvätkö ne varmistamaan kriittisten tai tärkeiden toimintojensa jatkuvuuden. Testauksen on täytettävä seuraavat vaatimukset:

a) se on suoritettava mahdollisia häiriöitä simuloivien testiskenaarioiden perusteella, mukaan lukien riittävä joukko vakavia mutta uskottavia skenaarioita;

b) siinä on tapauksen mukaan testattava TVT-palveluntarjoajana olevien kolmansien osapuolten tarjoamia TVT-palveluja;

c) asetuksen (EU) 2022/2554 11 artiklan 6 kohdan toisessa alakohdassa tarkoitettujen muiden kuin mikroyrityksiä olevien finanssiyhteisöjen osalta testaukseen on sisällytettävä skenaariot vaihtamisesta ensisijaisen TVT-infrastruktuurin ja varakapasiteetin, varmuuskopioiden ja varajärjestelmien välillä;

d) se on suunniteltava kyseenalaistamaan oletukset, joihin liiketoiminnan jatkuvuutta koskevat suunnitelmat perustuvat, mukaan lukien hallintojärjestelyt ja kriisiviestintäsuunnitelmat;

e) sen on sisällettävä menettelyt, joilla todennetaan finanssiyhteisöjen henkilöstön, TVT-palveluntarjoajana olevien kolmansien osapuolten, TVT-järjestelmien ja TVT-palvelujen kyky reagoida asianmukaisesti skenaarioihin, jotka on otettu asianmukaisesti huomioon 26 artiklan 2 kohdan mukaisesti.

Sovellettaessa a alakohtaa finanssiyhteisöjen on aina sisällytettävä testaukseen skenaariot, joita on tarkasteltu liiketoiminnan jatkuvuutta koskevia suunnitelmia laadittaessa.

Sovellettaessa b alakohtaa finanssiyhteisöjen on tarvittaessa otettava asianmukaisesti huomioon skenaariot, jotka liittyvät TVT-palveluntarjoajana olevien kolmansien osapuolten maksukyvyttömyyteen tai toimintahäiriöihin tai TVT-palveluntarjoajana olevien kolmansien osapuolten lainkäyttöalueilla esiintyviin poliittisiin riskeihin.

Kun sovelletaan c alakohtaa, testauksessa on todennettava, voidaanko ainakin kriittisiä tai tärkeitä toimintoja käyttää asianmukaisesti riittävän pitkän ajan ja voidaanko normaali toiminta palauttaa.

3. Edellä 2 kohdassa tarkoitettujen vaatimusten lisäksi keskusvastapuolten on otettava mukaan 1 kohdassa tarkoitettujen TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien testaukseen

a) määritysosapuolet;

b) ulkopuoliset palveluntarjoajat;

c) finanssi-infrastruktuuriin kuuluvat asiaankuuluvat laitokset, joiden kanssa keskusvastapuolet ovat havainneet keskinäisiä riippuvuussuhteita liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissaan.

4. Edellä 2 kohdassa tarkoitettujen vaatimusten lisäksi arvopaperikeskusten on otettava mukaan 1 kohdassa tarkoitettujen TVT-liiketoiminnan jatkuvuutta koskevien suunnitelmien testaukseen tapauksen mukaan

a) arvopaperikeskusten käyttäjät;

b) keskeisten yleishyödyllisten palvelujen ja muiden keskeisten palvelujen tarjoajat;

c) muut arvopaperikeskukset;

d) muut markkinainfrastruktuurit;

e) muut laitokset, joiden kanssa arvopaperikeskukset ovat havainneet keskinäisiä riippuvuussuhteita liiketoiminnan jatkuvuutta koskevissa toimintaperiaatteissaan.

5. Finanssiyhteisöjen on dokumentoitava 1 kohdassa tarkoitetun testauksen tulokset. Testauksessa havaitut puutteet on analysoitava, ne on korjattava ja niistä on ilmoitettava ylimmälle hallintoelimelle.

26 artikla

TVT-reagointi- ja palautumissuunnitelmat

1. Kun finanssiyhteisöt laativat asetuksen (EU) 2022/2554 11 artiklan 3 kohdassa tarkoitettuja TVT-reagointi- ja palautumissuunnitelmia, niiden on otettava huomioon finanssiyhteisön liiketoiminnan vaikutusanalyysin tulokset. TVT-reagointi- ja palautumissuunnitelmia koskevat seuraavat vaatimukset:

a) niissä on täsmennettävä edellytykset niiden aktivoinnille tai deaktivoinnille sekä mahdolliset aktivointia tai deaktivointia koskevat poikkeukset;

b) niissä on kuvattava, mitä toimia on toteutettava, jotta varmistetaan vähintään finanssiyhteisön kriittisiä tai tärkeitä toimintoja tukevien TVT-järjestelmien ja -palvelujen saatavuus, eheys, jatkuvuus ja palautuminen;

c) ne on suunniteltava siten, että ne täyttävät finanssiyhteisöjen toiminnan palautumistavoitteet;

d) ne on dokumentoitava ja asetettava TVT-reagointi- ja palautumissuunnitelmien täytäntöönpanoon osallistuvan henkilöstön saataville, ja niiden on oltava helposti saatavilla hätätilanteissa;

e) niissä on esitettävä vaihtoehtoja sekä lyhyen että pitkän aikavälin palautumiseen, mukaan lukien järjestelmien osittainen palautuminen;

f) niissä on vahvistettava TVT-reagointi- ja palautumissuunnitelmien tavoitteet sekä edellytykset, joilla suunnitelmien toteutus voidaan katsoa onnistuneeksi.

Sovellettaessa d alakohtaa finanssiyhteisöjen on määritettävä selkeästi tehtävät ja vastuut.

2. Edellä 1 kohdassa tarkoitetuissa TVT-reagointi- ja palautumissuunnitelmissa on määritettävä merkitykselliset skenaariot, mukaan lukien skenaariot vakavista liiketoiminnan häiriöistä ja kasvaneesta häiriön esiintymisen todennäköisyydestä. Suunnitelmissa on laadittava skenaarioita, jotka perustuvat ajantasaisiin tietoihin uhkista ja aiemmista liiketoiminnan häiriöistä saatuihin kokemuksiin. Finanssiyhteisöjen on otettava asianmukaisesti huomioon kaikki seuraavat skenaariot:

a) kyberhyökkäykset ja vaihtaminen ensisijaisen TVT-infrastruktuurin ja varakapasiteetin, varmuuskopioiden ja varajärjestelmien välillä;

b) skenaariot, joissa kriittisen tai tärkeän toiminnon laatu heikkenee kestämättömälle tasolle tai sen tarjoaminen lakkaa ja joissa otetaan asianmukaisesti huomioon asianomaisen TVT-palveluntarjoajana olevan kolmannen osapuolen maksukyvyttömyyden tai muun toimintahäiriön mahdolliset vaikutukset;

c) tilojen, mukaan lukien toimisto- ja liiketilat, ja datakeskusten osittaiset tai täydet toimintahäiriöt;

d) TVT-omaisuuden tai viestintäinfrastruktuurin merkittävä toimintahäiriö;

e) käytettävissä ei ole kriittistä määrää toiminnan jatkuvuuden takaamisesta vastaavaa henkilöstöä;

f) ilmastonmuutokseen ja ympäristön tilan heikkenemiseen liittyvien tapahtumien, luonnonkatastrofien, pandemioiden ja fyysisten hyökkäysten, mukaan lukien tunkeutuminen ja terrori-iskut, vaikutukset;

g) sisäpiirihyökkäykset;

h) poliittinen ja sosiaalinen epävakaus, tarvittaessa myös TVT-palveluntarjoajana olevan kolmannen osapuolen lainkäyttöalueella ja tietojen säilytys- ja käsittelypaikassa;

i) laajalle levinneet sähkökatkot.

3. Siltä varalta, että ensisijaiset palautumistoimenpiteet eivät välttämättä ole lyhyellä aikavälillä toteuttamiskelpoisia kustannusten, riskien, logistiikan tai odottamattomien olosuhteiden vuoksi, 1 kohdassa tarkoitetuissa TVT-reagointi- ja palautumissuunnitelmissa on tarkasteltava vaihtoehtoisia toimenpiteitä.

4. Finanssiyhteisöjen on osana 1 kohdassa tarkoitettuja TVT-reagointi- ja palautumissuunnitelmia tarkasteltava ja toteutettava toiminnan jatkuvuuden varmistamiseksi toimenpiteitä, joilla lievennetään finanssiyhteisön kriittisiä tai tärkeitä toimintoja tukevien TVT-palveluntarjoajana olevien kolmansien osapuolten toimintahäiriöiden vaikutuksia.

V LUKU

TVT-riskinhallintajärjestelmän uudelleentarkastelusta laadittava raportti

27 artikla

TVT-riskinhallinajärjestelmän uudelleentarkastelusta laadittavan raportin muoto ja sisältö

1. Finanssiyhteisöjen on toimitettava raportti asetuksen (EU) 2022/2554 6 artiklan 5 kohdassa tarkoitetusta TVT-riskinhallintajärjestelmän uudelleentarkastelusta haut mahdollistavassa sähköisessä muodossa.

2. Finanssiyhteisöjen on sisällytettävä 1 kohdassa tarkoitettuun raporttiin kaikki seuraavat tiedot:

a) johdanto-osa, jossa

i) yksilöidään selkeästi raportin kohteena oleva finanssiyhteisö ja kuvataan tarvittaessa sen konsernirakenne;

ii) kuvataan raportin taustaa finanssiyhteisön palvelujen, toimintojen ja toiminnan luonteen, laajuuden ja monimutkaisuuden, organisaation, yksilöityjen kriittisten toimintojen, strategian, merkittävien käynnissä olevien hankkeiden tai toimien sekä suhteiden osalta sekä finanssiyhteisön riippuvuutta sisäisistä ja sopimusperusteisista TVT-palveluista ja -järjestelmistä tai vaikutuksia, joita tällaisten järjestelmien täydellisellä keskeytymisellä tai vakavalla heikkenemisellä olisi kriittisiin tai tärkeisiin toimintoihin ja markkinoiden tehokkuuteen;

iii) esitetään yhteenveto TVT-riskinhallintajärjestelmässä edellisen raportin jälkeen tapahtuneista merkittävistä muutoksista;

iv) esitetään yhteenveto ajankohtaisesta ja lyhyen aikavälin TVT-riskiprofiilista, uhkaympäristöstä, finanssiyhteisön käyttämien valvontatoimien arvioidusta tehokkuudesta ja finanssiyhteisön turvallisuustasosta;

b) päivä, jona finanssiyhteisön ylin hallintoelin on hyväksynyt raportin;

c) kuvaus syistä TVT-riskinhallintajärjestelmän asetuksen (EU) 2022/2554 6 artiklan 5 kohdan mukaiseen uudelleen-tarkasteluun;

d) tarkastelujakson alkamis- ja päättymispäivä;

e) uudelleentarkastelusta vastaava toiminto;

f) kuvaus TVT-riskinhallintajärjestelmään edellisen uudelleentarkastelun jälkeen tehdyistä merkittävistä muutoksista ja parannuksista;

g) yhteenveto uudelleentarkastelun tuloksista sekä yksityiskohtainen analyysi ja arviointi TVT-riskinhallintajärjestelmän heikkouksien ja puutteiden vakavuudesta tarkastelujakson aikana;

h) kuvaus toimenpiteistä havaittujen heikkouksien ja puutteiden korjaamiseksi, mukaan lukien kaikki seuraavat:

   i) yhteenveto toimenpiteistä, joita on toteutettu havaittujen heikkouksien ja puutteiden korjaamiseksi;

   ii) toimenpiteiden arvioitu täytäntöönpanopäivä ja täytäntöönpanon sisäiseen valvontaan liittyvät päivämäärät, mukaan lukien tiedot kyseisten toimenpiteiden täytäntöönpanon edistymisestä raportin laatimispäivänä ja tarvittaessa selvitys siitä, onko vaarana, että määräaikoja ei voida noudattaa;

   iii) käytettävät välineet ja toimenpiteiden toteuttamisesta vastaavan toiminnon määrittäminen sekä se, ovatko välineet ja toiminnot sisäisiä vai ulkoisia;

   iv) kuvaus toimenpiteissä suunniteltujen muutosten vaikutuksesta finanssiyhteisön varoihin sekä henkilöstö- ja aineellisiin resursseihin, mukaan lukien mahdollisten korjaavien toimenpiteiden toteuttamiseen tarkoitetut resurssit;

   v) tiedot menettelystä, jolla toimivaltaisia viranomaisia informoidaan tarvittaessa;

   vi) jos havaittuihin heikkouksiin tai puutteisiin ei sovelleta korjaavia toimenpiteitä, yksityiskohtainen selvitys kriteereistä, joita on käytetty kyseisten heikkouksien tai puutteiden vaikutusten analysoinnissa sekä niihin liittyvän TVT-jäännösriskin arvioinnissa, ja perusteista, joita on käytetty jäännösriskin hyväksymiseen;

i) TVT-riskinhallintajärjestelmän suunniteltu jatkokehitys;

j) TVT-riskinhallintajärjestelmän uudelleentarkastelun tuloksena saadut päätelmät;

k) tiedot aiemmista uudelleentarkasteluista, mukaan lukien

   i) luettelo kaikista aiemmin tehdyistä tarkasteluista;

   ii) tapauksen mukaan edellisessä raportissa yksilöityjen korjaavien toimenpiteiden täytäntöönpanon tilanne;

   iii) jos aiemmissa uudelleentarkasteluissa ehdotetut korjaavat toimenpiteet ovat osoittautuneet tehottomiksi tai ne ovat aiheuttaneet odottamattomia haasteita, kuvaus siitä, miten korjaavia toimenpiteitä voitaisiin parantaa, tai kuvaus odottamattomista haasteista;

l) raportin laatimisessa käytetyt tietolähteet, mukaan lukien kaikki seuraavat:

   i) asetuksen (EU) 2022/2554 6 artiklan 6 kohdassa tarkoitettujen muiden kuin mikroyrityksiä olevien finanssiyhteisöjen osalta sisäisten tarkastusten tulokset;

   ii) vaatimusten noudattamisen arvioinnin tulokset;

   iii) TVT-välineiden, -järjestelmien ja -prosessien digitaalisen häiriönsietokyvyn testauksen tulokset ja tarvittaessa uhkavetoiseen tunkeutumistestaukseen perustuvan kehittyneen testauksen tulokset;

   iv) ulkopuoliset lähteet.

Sovellettaessa c alakohtaa, jos uudelleentarkastelu käynnistettiin valvontaohjeiden tai asiaankuuluvista digitaalisen häiriönsietokyvyn testauksesta tai auditointiprosesseista johdettujen päätelmien mukaisesti, raportissa on oltava viittaus tällaisiin ohjeisiin tai päätelmiin, jotta uudelleentarkastelun aloittamisen syy voidaan määrittää. Jos uudelleentarkastelu käynnistettiin TVT:hen liittyvien poikkeamien seurauksena, raportin on sisällettävä luettelo kaikista TVT:hen liittyvistä poikkeamista sekä analyysi poikkeamien juurisyistä.

Sovellettaessa f alakohtaa kuvauksen on sisällettävä analyysi muutosten vaikutuksista finanssiyhteisön digitaalisen häiriönsietokyvyn strategiaan, finanssiyhteisön TVT:n sisäisen valvonnan kehykseen ja finanssiyhteisön TVT-riskinhallinnan hallintorakenteeseen.

III OSASTO

ASETUKSEN (EU) 2022/2554 16 ARTIKLAN 1 KOHDASSA TARKOITETTUJEN FINANSSIYHTEISÖJEN YKSINKERTAISTETTU TVT-RISKINHALLINTAJÄRJESTELMÄ

I LUKU

Yksinkertaistettu TVT-riskinhallintajärjestelmä

28 artikla

Hallinto ja organisaatio

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitetuilla finanssiyhteisöillä on oltava käytössään sisäinen hallinto- ja valvontakehys, jolla varmistetaan tehokas ja vakaa TVT-riskinhallinta digitaalisen häiriönsietokyvyn korkean tason saavuttamiseksi.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on osana yksinkertaistettua TVT-riskinhallintajärjestelmäänsä varmistettava, että niiden ylin hallintoelin

a) kantaa kokonaisvastuun sen varmistamisesta, että yksinkertaistettu TVT-riskinhallintajärjestelmä mahdollistaa finanssiyhteisön liiketoimintastrategian toteuttamisen kyseisen finanssiyhteisön riskinottohalun mukaisesti, ja varmistaa, että TVT-riski otetaan huomioon tässä yhteydessä;

b) asettaa kaikille TVT:hen liittyville toimille selkeät tehtävä- ja vastuualueet;

c) vahvistaa tietoturvatavoitteet ja TVT-vaatimukset;

d) hyväksyy, valvoo ja tarkistaa säännöllisesti

   i) tämän asetuksen 30 artiklan 1 kohdassa tarkoitetun finanssiyhteisön tieto-omaisuuden luokituksen, luettelon tärkeimmistä tunnistetuista riskeistä sekä liiketoiminnan vaikutusanalyysin ja siihen liittyvät toimintaperiaatteet;

   ii) finanssiyhteisön liiketoiminnan jatkuvuussuunnitelmat sekä asetuksen (EU) 2022/2554 16 artiklan 1 kohdan f alakohdassa tarkoitetut reagointi- ja toipumistoimenpiteet;

e) osoittaa tarvittavat määrärahat, jotta finanssiyhteisön digitaalisen häiriönsietokyvyn tarpeet voidaan täyttää kaikkien eri resurssityyppien osalta, mukaan lukien asianmukaiset TVT-turvallisuutta koskevat valistusohjelmat ja digitaalista häiriönsietokykyä käsittelevä koulutus sekä koko henkilöstön TVT-osaaminen, ja tarkastelee niitä uudelleen vähintään kerran vuodessa;

f) täsmentää ja panee täytäntöön tämän osaston I, II ja III lukuun sisältyvät toimintaperiaatteet ja toimenpiteet, jotta voidaan tunnistaa, arvioida ja hallita TVT-riskiä, jolle finanssiyhteisö altistuu;

g) määrittää ja toteuttaa menettelyt, TVT-protokollat ja välineet, jotka ovat tarpeen kaiken tieto-omaisuuden ja TVT-omaisuuden suojaamiseksi;

h) varmistaa, että finanssiyhteisön henkilöstö pidetään ajan tasalla ja että sillä on riittävät ja hallinnoitavaan TVT-riskiin nähden oikeasuhteiset tiedot ja taidot ymmärtää ja arvioida TVT-riskiä ja sen vaikutusta finanssiyhteisön toimintaan;

i) vahvistaa järjestelyt tietoturvallisuutta ja digitaalista häiriönsietokykyä koskevalle raportoinnille ylimmälle hallintoelimelle, mukaan lukien raportoinnin tiheys, muoto ja sisältö.

3. Edellä 1 kohdassa tarkoitetut finanssiyhteisöt voivat unionin ja kansallisen alakohtaisen lainsäädännön mukaisesti ulkoistaa TVT-riskinhallintavaatimusten noudattamisen todentamistehtävät konsernin sisäisille TVT-palveluntarjoajille tai TVT-palveluntarjoajana oleville kolmansille osapuolille. Tällaisen ulkoistamisen tapauksessa finanssiyhteisöt ovat edelleen täysin vastuussa TVT-riskinhallintavaatimusten noudattamisen todentamisesta.

4. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on varmistettava valvontatoimintojen ja sisäisen tarkastuksen toimintojen asianmukainen erottelu ja riippumattomuus.

5. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on varmistettava, että niiden yksinkertaistetusta TVT-riskinhallintajärjestelmästä tehdään auditoijien sisäinen tarkastus finanssiyhteisöjen auditointisuunnitelman mukaisesti. Auditoijilla on oltava riittävät tiedot, taidot ja asiantuntemus TVT-riskeistä ja heidän on oltava riippumattomia. TVT-auditointien tiheys ja painopisteet on määritettävä finanssiyhteisön TVT-riskiä vastaavasti.

6. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on 5 kohdassa tarkoitetun auditoinnin tulosten perusteella varmistettava TVT-auditoinnin kriittisten havaintojen pikainen todentaminen ja korjaaminen.

29 artikla

Tietoturvapolitiikka ja -toimenpiteet

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on osana yksinkertaistettua TVT-riskinhallintajärjestelmää laadittava, dokumentoitava ja pantava täytäntöön tietoturvapolitiikka. Tietoturvapolitiikassa on täsmennettävä korkean tason periaatteet ja säännöt, joilla suojataan tietojen ja finanssiyhteisöjen tarjoamien palvelujen luottamuksellisuutta, eheyttä, saatavuutta ja aitoutta.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on 1 kohdassa tarkoitetun tietoturvapolitiikkansa perusteella laadittava ja toteutettava TVT-turvallisuutta koskevia toimenpiteitä, mukaan lukien TVT-palveluntarjoajana olevien kolmansien osapuolten toteuttamat lieventävät toimenpiteet, joilla lievennetään niiden altistumista TVT-riskille.

TVT-turvallisuutta koskeviin toimenpiteisiin on sisällyttävä kaikki 30–38 artiklassa tarkoitetut toimenpiteet.

30 artikla

Tieto-omaisuuden ja TVT-omaisuuden luokittelu

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on osana kyseisen 1 kohdan a alakohdassa tarkoitettua yksinkertaistettua TVT-riskinhallintajärjestelmää yksilöitävä, luokiteltava ja dokumentoitava kaikki kriittiset tai tärkeät toiminnot, niitä tukeva tieto- ja TVT-omaisuus sekä niiden keskinäiset riippuvuussuhteet. Finanssiyhteisöjen on tarkasteltava tätä yksilöintiä ja luokittelua uudelleen tarpeen mukaan.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on yksilöitävä kaikki TVT-palveluntarjoajana olevien kolmansien osapuolten tukemat kriittiset tai tärkeät toiminnot.

31 artikla

TVT-riskienhallinta

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on sisällytettävä yksinkertaistettuun TVT-riskinhallintajärjestelmäänsä kaikki seuraavat:

a) TVT-riskitasojen määrittäminen finanssiyhteisön riskinottohalun mukaisesti;

b) niiden TVT-riskien tunnistaminen ja arviointi, joille finanssiyhteisö altistuu;

c) lieventämisstrategioiden määrittely ainakin sellaisten TVT-riskien osalta, jotka eivät ole finanssiyhteisön riskirajojen sisällä;

d) edellä c alakohdassa tarkoitettujen lieventämisstrategioiden tehokkuuden seuranta;

e) sellaisten TVT- ja tietoturvariskien tunnistaminen ja arviointi, jotka johtuvat TVT-järjestelmissä, -palveluissa, -prosesseissa tai -menettelyissä tapahtuneista merkittävistä muutoksista ja jotka on havaittu TVT-turvallisuustestauksen tuloksena ja mahdollisten laajavaikutteisten TVT:hen liittyvien poikkeamien jälkeen.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on suoritettava ja dokumentoitava määräajoin TVT-riskinarviointi, joka on oikeassa suhteessa finanssiyhteisöjen TVT-riskiprofiiliin.

3. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on jatkuvasti seurattava uhkia ja haavoittuvuuksia, jotka ovat merkityksellisiä niiden kriittisten tai tärkeiden toimintojen, tieto-omaisuuden ja TVT-omaisuuden kannalta, ja tarkasteltava säännöllisesti uudelleen kyseisiin kriittisiin tai tärkeisiin toimintoihin vaikuttavia riskiskenaarioita.

4. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on vahvistettava varoituskynnykset ja kriteerit, jotka käynnistävät TVT:hen liittyviä poikkeamia koskevat reagointiprosessit.

32 artikla

Fyysinen turvallisuus ja ympäristön turvallisuus

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on määritettävä ja toteutettava fyysiset turvatoimenpiteet, jotka on suunniteltu uhkaympäristön, tämän asetuksen 30 artiklan 1 kohdassa tarkoitetun luokittelun, TVT-omaisuuden yleisen riskiprofiilin ja saatavilla olevan tieto-omaisuuden perusteella.

2. Edellä 1 kohdassa tarkoitetuilla toimenpiteillä on suojattava finanssiyhteisöjen tilat ja tapauksen mukaan sellaiset finanssiyhteisöjen datakeskukset, joissa on TVT-omaisuutta ja tieto-omaisuutta, luvattomalta pääsyltä, hyökkäyksiltä ja onnettomuuksilta sekä ympäristöuhkilta ja -vaaroilta.

3. Ympäristöuhkilta ja -vaaroilta suojautumisen on oltava oikeassa suhteessa tilojen ja tapauksen mukaan datakeskusten merkitykseen sekä niissä sijaitsevien toimintojen tai TVT-järjestelmien kriittisyyteen.

II LUKU

Muut järjestelmien, protokollien ja välineiden osatekijät, joilla minimoidaan TVT-riskien vaikutusta

33 artikla

Pääsynvalvonta

Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on laadittava, dokumentoitava ja otettava käyttöön loogisen ja fyysisen pääsynvalvonnan menettelyt ja valvottava, seurattava ja tarkasteltava niitä säännöllisesti. Menettelyihin on sisällyttävä seuraavat loogisen ja fyysisen pääsynvalvonnan osatekijät:

a) tieto-omaisuuteen, TVT-omaisuuteen ja niillä tuettuihin toimintoihin sekä finanssiyhteisön kriittisiin toimipaikkoihin liittyviä pääsyoikeuksia, mukaan lukien etäkäyttöoikeudet ja hätätilanteen käyttöoikeudet, hallinnoidaan tiedonsaantitarpeen, käyttötarpeen ja vähäisimpien oikeuksien periaatteiden mukaisesti;

b) käyttäjien vastuuvelvollisuus, jolla varmistetaan, että käyttäjät voidaan tunnistaa TVT-järjestelmissä tapahtuvan toiminnan osalta;

c) tilinhallintamenettelyt käyttäjätilien ja yleisten tilien, mukaan lukien yleisten pääkäyttäjätilien, käyttöoikeuksien myöntämiseksi, muuttamiseksi tai peruuttamiseksi;

d) todentamismenetelmät, jotka ovat oikeassa suhteessa 30 artiklan 1 kohdassa tarkoitettuun luokitteluun ja TVT-omaisuuden yleiseen riskiprofiiliin ja jotka perustuvat johtaviin käytäntöihin;

e) käyttöoikeuksia tarkistetaan säännöllisesti uudelleen, ja ne peruutetaan, kun niitä ei enää tarvita.

Sovellettaessa c alakohtaa finanssiyhteisön on myönnettävä erityis-, hätätilanne- ja järjestelmävastaavan oikeudet kaikkiin TVT-järjestelmiin käyttötarpeen perusteella tai tapauskohtaisesti, ja asia on kirjattava lokitietoihin 34 artiklan ensimmäisen kohdan f alakohdan mukaisesti.

Sovellettaessa d alakohtaa finanssiyhteisöjen on käytettävä johtaviin käytäntöihin perustuvia vahvan tunnistuksen menetelmiä siltä osin kuin on kyse etäyhteyden ottamisesta finanssiyhteisöjen verkkoon, erityisoikeuksista ja julkisesti saatavilla olevia kriittisiä tai tärkeitä toimintoja tukevan TVT-omaisuuden käyttöoikeuksista.

34 artikla

TVT-toimien turvallisuus

Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on osana järjestelmiään, protokolliaan ja välineitään sekä kaiken TVT-omaisuuden osalta

a) seurattava ja hallittava kaiken TVT-omaisuuden elinkaarta;

b) seurattava tarvittaessa, tukevatko finanssiyhteisöjen TVT-palveluntarjoajana olevat kolmannet osapuolet niiden TVT-omaisuutta;

c) määritettävä TVT-omaisuutensa kapasiteettivaatimukset ja toimenpiteet, joilla ylläpidetään ja parannetaan TVT-järjestelmien saatavuutta ja tehokkuutta ja ennaltaehkäistään TVT-kapasiteettivajeita;

d) suoritettava TVT-omaisuuden automatisoitu haavoittuvuuskartoitus ja automatisoidut arvioinnit, jotka ovat oikeassa suhteessa niiden 30 artiklan 1 kohdassa tarkoitettuun luokitteluun ja TVT-omaisuuden yleiseen riskiprofiiliin, ja paikattava havaitut haavoittuvuudet korjauspäivityksillä;

e) hallittava vanhentuneeseen, tukemattomaan tai aiemman sukupolven TVT-omaisuuteen liittyviä riskejä;

f) kirjattava lokiin tapahtumat, jotka liittyvät loogiseen ja fyysiseen pääsynvalvontaan, TVT-toimiin, mukaan lukien järjestelmä- ja verkkoliikennetoiminnot, ja TVT-muutosten hallintaan;

g) määritettävä ja toteutettava toimenpiteitä, joilla seurataan ja analysoidaan tietoja poikkeavasta toiminnasta ja käyttäytymisestä kriittisissä tai tärkeissä TVT-toimissa;

h) toteutettava toimenpiteitä kyberuhkia koskevien merkityksellisten ja ajantasaisten tietojen seuraamiseksi;

i) toteutettava toimenpiteitä, joilla tunnistetaan mahdolliset tietovuodot, haitalliset koodit ja muut turvallisuusuhat sekä yleisesti tunnetut haavoittuvuudet ohjelmistoissa ja laitteistoissa, ja tarkistetaan, onko niihin liittyen saatavilla uusia turvallisuuspäivityksiä.

Sovellettaessa f alakohtaa finanssiyhteisöjen on sovitettava lokitietojen yksityiskohtaisuus niiden käyttötarkoitukseen ja kyseiset lokitiedot tuottavan TVT-omaisuuden käyttötarkoitukseen.

35 artikla

Tietojen, järjestelmän ja verkon turvallisuus

Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on osana järjestelmiään, protokolliaan ja välineitään laadittava ja otettava käyttöön suojatoimia, joilla varmistetaan verkkojen turvallisuus tunkeutumiselta ja datan väärinkäytöltä ja joilla säilytetään tietojen saatavuus, aitous, eheys ja luottamuksellisuus. Finanssiyhteisöjen on erityisesti vahvistettava kaikki seuraavat seikat ottaen huomioon tämän asetuksen 30 artiklan 1 kohdassa tarkoitetun luokittelun:

a) tietojen suojaamista käsittelyn ja siirtämisen aikana sekä levossa koskevien toimenpiteiden määrittäminen ja toteuttaminen;

b) finanssiyhteisön tietojen siirtämiseen ja tallentamiseen käytettävien ohjelmistojen, tallennusvälineiden, järjestelmien ja päätelaitteiden käyttöä koskevien turvatoimenpiteiden määrittäminen ja toteuttaminen;

c) sellaisten toimenpiteiden määrittäminen ja toteuttaminen, joilla estetään ja havaitaan luvattomat yhteydet finanssiyhteisön verkkoon sekä suojataan finanssiyhteisön sisäisten verkkojen sekä internetin ja muiden ulkoisten yhteyksien välinen verkkoliikenne;

d) sellaisten toimenpiteiden määrittäminen ja toteuttaminen, joilla varmistetaan tietojen saatavuus, aitous, eheys ja luottamuksellisuus verkossa tapahtuvan siirron aikana;

e) menettely, jolla toimitiloissa tai ulkoisesti tallennetut tiedot, joita finanssiyhteisön ei enää tarvitse kerätä tai tallentaa, poistetaan turvallisesti;

f) menettely, jolla toimitiloissa tai ulkoisesti säilytettävät luottamuksellisia tietoja sisältävät tallennuslaitteet hävitetään tai poistetaan käytöstä turvallisesti;

g) sellaisten toimenpiteiden määrittäminen ja toteuttaminen, joilla varmistetaan, että etätyö ja yksityisten päätelaitteiden käyttö eivät vaikuta kielteisesti finanssiyhteisön kykyyn suorittaa kriittisiä toimintojaan asianmukaisella, oikea-aikaisella ja turvallisella tavalla.

36 artikla

TVT-turvallisuuden testaus

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on laadittava ja pantava täytäntöön TVT-turvallisuuden testaussuunnitelma tämän asetuksen 33, 34 ja 35 artiklan sekä 37 ja 38 artiklan mukaisesti kehitettyjen TVT-turvallisuustoimenpiteidensä tehokkuuden todentamiseksi. Finanssiyhteisöjen on varmistettava, että suunnitelmassa otetaan huomioon uhat ja haavoittuvuudet, jotka on tunnistettu osana tämän asetuksen 31 artiklassa tarkoitettua yksinkertaistettua TVT-riskinhallintajärjestelmää.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on tarkasteltava, arvioitava ja testattava TVT-turvallisuustoimenpiteitä ottaen huomioon finanssiyhteisön TVT-omaisuuden yleisen riskiprofiilin.

3. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on seurattava ja arvioitava turvallisuustestien tuloksia ja saatettava kriittisiä tai tärkeitä toimintoja tukevia TVT-järjestelmiä koskevat turvatoimenpiteensä ajan tasalle ilman aiheetonta viivytystä.

37 artikla

TVT-järjestelmien hankinta, kehittäminen ja ylläpito

Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on tarvittaessa laadittava ja toteutettava TVT-järjestelmien hankintaa, kehittämistä ja ylläpitoa koskeva menettely riskiperusteista lähestymistapaa noudattaen. Menettelyllä on

a) varmistettava, että ennen TVT-järjestelmien hankintaa tai kehittämistä asiaan liittyvä liiketoiminto määrittelee ja hyväksyy toiminnalliset ja muut vaatimukset, mukaan lukien tietoturvavaatimukset;

b) varmistettava, että TVT-järjestelmät testataan ja hyväksytään ennen niiden ensimmäistä käyttöä ja ennen kuin tuotantoympäristöön tehdään muutoksia;

c) määritettävä toimenpiteet, joilla tuotantoympäristössä tapahtuvan kehittämisen ja käyttöönoton aikana lievennetään riskiä kyseisten TVT-järjestelmien tahattomasta muuttamisesta tai tarkoituksellisesta manipuloinnista.

38 artikla

TVT-hankkeiden ja -muutosten hallinta

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on laadittava, dokumentoitava ja otettava käyttöön TVT-hankkeiden hallintamenettely ja määritettävä tehtävät ja vastuut sen täytäntöönpanossa. Menettelyn on katettava TVT-hankkeiden kaikki vaiheet niiden käynnistämisestä niiden päättämiseen.

2. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on laadittava, dokumentoitava ja otettava käyttöön TVT-muutosten hallintamenettely, jolla varmistetaan, että kaikki TVT-järjestelmien muutokset kirjataan, testataan, arvioidaan, hyväksytään, toteutetaan ja todennetaan valvotulla tavalla ja että finanssiyhteisön digitaalinen häiriönsietokyky suojataan asianmukaisin suojatoimin.

III LUKU

TVT-liiketoiminnan jatkuvuuden hallinta

39 artikla

TVT-liiketoiminnan jatkuvuutta koskevan suunnitelman osatekijät

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on laadittava TVT-toiminnan jatkuvuutta koskevat suunnitelmansa ottaen huomioon tulokset analyyseistä, jotka koskevat niiden altistumista vakaville liiketoiminnan häiriöille ja tällaisten häiriöiden mahdollisia vaikutuksia, sekä skenaariot, joille niiden kriittisiä tai tärkeitä toimintoja tukeva TVT-omaisuus saattaa altistua, mukaan lukien kyberhyökkäysskenaario.

2. Edellä 1 kohdassa tarkoitettuihin liiketoiminnan jatkuvuutta koskeviin suunnitelmiin sovelletaan seuraavia edellytyksiä:

a) finanssiyhteisön ylimmän hallintoelimen on hyväksyttävä ne;

b) ne on dokumentoitava ja niiden on oltava helposti saatavilla hätä- ja kriisitilanteessa;

c) niiden toteuttamiseen on osoitettava riittävät resurssit;

d) niissä on vahvistettava suunnitellut palautumistasot ja aikataulut toimintojen ja keskeisten sisäisten ja ulkoisten riippuvuuksien palautumiselle ja jatkumiselle, mukaan lukien TVT-palveluntarjoajana olevien kolmansien osapuolten osalta;

e) niissä on määritettävä olosuhteet, jotka voivat johtaa TVT-liiketoiminnan jatkuvuussuunnitelmien aktivoimiseen, ja toimet, joita on toteutettava kriittisiä tai tärkeitä toimintoja tukevan finanssiyhteisöjen TVT-omaisuuden saatavuuden, jatkuvuuden ja palautumisen varmistamiseksi;

f) niissä on määritettävä kriittisten tai tärkeiden liiketoimintojen, tukiprosessien, tieto-omaisuuden ja niiden keskinäisten riippuvuuksien palauttamis- ja palautumistoimenpiteet, jotta vältetään haitalliset vaikutukset finanssiyhteisöjen toimintaan;

g) niissä on määritettävä varmuuskopiointimenettelyt ja -toimenpiteet, joissa määritetään varmuuskopioitavat tiedot ja varmuuskopioinnin vähimmäistiheys kyseisiä tietoja käyttävän toiminnon kriittisyyden perusteella;

h) niissä on tarkasteltava vaihtoehtoja sellaisia tapauksia varten, joissa palautuminen ei ehkä ole lyhyellä aikavälillä toteutettavissa kustannusten, riskien, logistiikan tai ennakoimattomien olosuhteiden vuoksi;

i) niissä on täsmennettävä sisäiset ja ulkoiset viestintäjärjestelyt, mukaan lukien eskalaatiosuunnitelmat;

j) ne on päivitettävä poikkeamista, testeistä, uusista riskeistä ja tunnistetuista uhkista saatujen kokemusten, muuttuneiden elpymistavoitteiden sekä finanssiyhteisön organisaatioon ja kriittisiä toimintoja tai liiketoimintoja tukevaan TVT-omaisuuteen tehtyjen merkittävien muutosten perusteella.

Sovellettaessa f alakohtaa kyseisessä alakohdassa tarkoitetuilla toimenpiteillä on voitava lieventää kriittisten palveluntarjoajana olevien kolmansien osapuolten toimintahäiriöitä.

40 artikla

Liiketoiminnan jatkuvuutta koskevien suunnitelmien testaus

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on testattava tämän asetuksen 39 artiklassa tarkoitetut liiketoiminnan jatkuvuutta koskevat suunnitelmansa, mukaan lukien kyseisessä artiklassa tarkoitetut skenaariot, vähintään kerran vuodessa varmuuskopiointi- ja palautusmenettelyjen osalta ja jokaisen liiketoiminnan jatkuvuutta koskevaan suunnitelmaan tehtävän merkittävän muutoksen yhteydessä.

2. Edellä 1 kohdassa tarkoitetussa liiketoiminnan jatkuvuutta koskevien suunnitelmien testauksessa on osoitettava, että kyseisessä kohdassa tarkoitetut finanssiyhteisöt pystyvät ylläpitämään liiketoimintaansa, kunnes kriittiset toiminnot on palautettu, ja tunnistamaan kyseisissä suunnitelmissa mahdollisesti olevat puutteet.

3. Edellä 1 kohdassa tarkoitettujen finanssiyhteisöjen on dokumentoitava liiketoiminnan jatkuvuutta koskevien suunnitelmien testauksen tulokset, ja testauksessa havaitut puutteet on analysoitava, käsiteltävä ja niistä on raportoitava ylimmälle hallintoelimelle.

IV LUKU

Yksinkertaistetun TVT-riskinhallintajärjestelmän uudelleentarkastelua koskeva raportti

41 artikla

Yksinkertaistetun TVT-riskinhallinajärjestelmän uudelleentarkastelua koskevan raportin muoto ja sisältö

1. Asetuksen (EU) 2022/2554 16 artiklan 1 kohdassa tarkoitettujen finanssiyhteisöjen on toimitettava raportti mainitun artiklan 2 kohdassa tarkoitetusta TVT-riskinhallintajärjestelmän uudelleentarkastelusta haut mahdollistavassa sähköisessä muodossa.

2. Edellä 1 kohdassa tarkoitetun raportin on sisällettävä kaikki seuraavat tiedot:

a) johdanto-osa, jossa

   i) kuvataan raportin taustaa finanssiyhteisön palvelujen, toimintojen ja toiminnan luonteen, laajuuden ja monimutkaisuuden, finanssiyhteisön organisaation, yksilöityjen kriittisten toimintojen, strategian, merkittävien käynnissä olevien hankkeiden tai toimien sekä suhteiden osalta sekä finanssiyhteisön riippuvuutta sisäisistä ja ulkoistetuista TVT-palveluista ja -järjestelmistä tai vaikutuksia, joita tällaisten järjestelmien täydellisellä keskeytymisellä tai vakavalla heikkenemisellä olisi kriittisiin tai tärkeisiin toimintoihin ja markkinoiden tehokkuuteen;

   ii) esitetään yhteenveto tunnistetuista ajankohtaisista ja lyhyen aikavälin TVT-riskeistä, uhkaympäristöstä, finanssiyhteisön käyttämien valvontatoimien arvioidusta tehokkuudesta ja finanssiyhteisön turvallisuustasosta;

   iii) esitetään tiedot raportoinnin kohteena olevasta osa-alueesta;

   iv) esitetään yhteenveto TVT-riskinhallintajärjestelmässä edellisen raportin jälkeen tapahtuneista merkittävistä muutoksista;

   v) esitetään yhteenveto ja kuvaus yksinkertaistettuun TVT-riskinhallintajärjestelmään edellisen raportin jälkeen tehtyjen muutosten vaikutuksista;

b) tapauksen mukaan päivä, jona finanssiyhteisön ylin hallintoelin on hyväksynyt raportin;

c) kuvaus uudelleentarkastelun syistä, mukaan lukien

   i) jos uudelleentarkastelu on käynnistetty valvontaohjeiden perusteella, näyttö kyseisistä ohjeista;

   ii) jos uudelleentarkastelu on käynnistetty TVT:hen liittyvien poikkeamien vuoksi, luettelo kaikista näistä TVT:hen liittyvistä poikkeamista sekä analyysi niiden perimmäisistä syistä;

d) tarkastelujakson alkamis- ja päättymispäivä;

e) raportista vastaavan henkilön nimi;

f) yhteenveto havainnoista sekä itsearviointi TVT-riskinhallintajärjestelmässä tarkastelujaksolla havaittujen heikkouksien ja puutteiden vakavuudesta, mukaan lukien näiden yksityiskohtainen analyysi;

g) yksinkertaistetun TVT-riskinhallintajärjestelmän heikkouksien ja puutteiden korjaamiseksi määritetyt toimenpiteet ja näiden toimenpiteiden odotettu täytäntöönpanopäivä, mukaan lukien tiedot edistymisestä aiemmissa raporteissa yksilöityjen heikkouksien ja puutteiden korjaamisessa, jos näitä heikkouksia ja puutteita ei ole vielä korjattu;

h) yleiset päätelmät yksinkertaistetun TVT-riskinhallintajärjestelmän uudelleentarkastelusta, mukaan lukien suunnitellut jatkotoimet.

IV OSASTO

LOPPUSÄÄNNÖKSET

42 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 13 päivänä maaliskuuta 2024.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN