

RICHTLIJN (EU) 2022/2556 VAN HET EUROPEES PARLEMENT EN DE RAAD**van 14 december 2022****tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector****(Voor de EER relevante tekst)**

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name de artikelen 53, lid 1, en 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van de Europese Centrale Bank ⁽¹⁾,

Gezien het advies van het Europees Economisch en Sociaal Comité ⁽²⁾,

Handelend volgens de gewone wetgevingsprocedure ⁽³⁾,

Overwegende hetgeen volgt:

- (1) De Unie moet zorgen voor een passende en alomvattende aanpak van de digitale risico's voor alle financiële entiteiten die voortvloeien uit een toegenomen gebruik van informatie- en communicatietechnologie (ICT) bij de verstrekking en het verbruik van financiële diensten, en daarbij bijdragen aan de verwezenlijking van het potentieel van digitale financiering, door innovatie te stimuleren en mededinging in een veilige digitale omgeving te bevorderen.
- (2) Financiële entiteiten zijn sterk afhankelijk van het gebruik van digitale technologieën in hun dagelijkse activiteiten. Het is daarom van het grootste belang dat de operationele weerbaarheid van hun digitale operaties tegen ICT-risico's gewaarborgd blijft. Dit is des te belangrijker vanwege de groei van baanbrekende technologieën in de markt, met name technologieën waardoor het mogelijk wordt digitale weergaven van waarde of rechten elektronisch over te dragen en te bewaren met behulp van distributed ledger of soortgelijke technologie (cryptoactiva), en de groei van diensten die met die activa verband houden.

⁽¹⁾ PB C 343 van 26.8.2021, blz. 1.

⁽²⁾ PB C 155 van 30.4.2021, blz. 38.

⁽³⁾ Standpunt van het Europees Parlement van 10 november 2022 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 28 november 2022.

- (3) Vereisten betreffende het beheer van het ICT-risico in de financiële sector zijn op het niveau van de Unie momenteel vastgelegd in de Richtlijnen 2009/65/EG⁽⁴⁾, 2009/138/EG⁽⁵⁾, 2011/61/EU⁽⁶⁾, 2013/36/EU⁽⁷⁾, 2014/59/EU⁽⁸⁾, 2014/65/EU⁽⁹⁾, (EU) 2015/2366⁽¹⁰⁾ en (EU) 2016/2341⁽¹¹⁾ van het Europees Parlement en de Raad. Die vereisten zijn erg uiteenlopend en soms onvolledig.

In een aantal gevallen is het ICT-risico slechts impliciet aangepakt als onderdeel van het operationele risico, en in andere gevallen zelfs helemaal niet. Die problemen worden verholpen door de vaststelling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad⁽¹²⁾. De voornoemde richtlijnen moeten derhalve worden gewijzigd om ze in overeenstemming te brengen met die verordening. Deze richtlijn bevat een reeks wijzigingen die noodzakelijk zijn om te zorgen voor juridische duidelijkheid en consistentie indien financiële entiteiten waaraan vergunningen werden verleend en waarop toezicht wordt uitgeoefend overeenkomstig die richtlijnen, diverse vereisten inzake digitale operationele weerbaarheid toepassen die nodig zijn voor de uitoefening hun activiteiten en voor de verrichting van diensten, zodat de goede werking van de interne markt wordt gewaarborgd. Er moet voor worden gezorgd dat die vereisten aansluiten bij de marktontwikkelingen en tegelijkertijd de proportionaliteit aanmoedigen, met name wat betreft de omvang van de financiële entiteiten en de specifieke regelgeving waaraan zij onderworpen zijn, met als doel de nalevingskosten te verminderen.

- (4) Op het gebied van bankdiensten bevat Richtlijn 2013/36/EU momenteel enkel algemene interne governanceregels en operationeelrisicobepalingen met vereisten voor nood- en bedrijfscontinuïteitsplannen, die impliciet als basis dienen voor ICT-risicobeheer. Om het ICT-risico echter expliciet en duidelijk aan te pakken, moeten de vereisten voor nood- en bedrijfscontinuïteitsplannen worden gewijzigd om daarin ook bedrijfscontinuïteitsplannen en respons- en herstelplannen voor het ICT-risico op te nemen, in overeenstemming met de vereisten van Verordening (EU) 2022/2554. Bovendien is het ICT-risico slechts impliciet opgenomen, als onderdeel van het operationele risico, in de procedure voor toetsing en evaluatie door de toezichthouder (*Supervisory Review and Evaluation Process* — SREP) die de bevoegde autoriteiten uitvoeren, en zijn de criteria voor de beoordeling van het ICT-risico momenteel vastgelegd in de Richtsnoeren inzake de beoordeling van het ICT-risico in het kader van het proces van toetsing en evaluatie door de toezichthouder (SREP), uitgevaardigd door de Europese toezichthoudende autoriteit (Europese Bankautoriteit) (EBA), die is opgericht bij Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad⁽¹³⁾. Om juridische duidelijkheid te scheppen en ervoor te zorgen dat banktoezichthouders het ICT-risico effectief vaststellen en het beheer ervan door financiële entiteiten monitoren, in overeenstemming met het nieuwe

⁽⁴⁾ Richtlijn 2009/65/EG van het Europees Parlement en de Raad van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe's) (PB L 302 van 17.11.2009, blz. 32).

⁽⁵⁾ Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1).

⁽⁶⁾ Richtlijn 2011/61/EU van het Europees Parlement en de Raad van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 1095/2010 (PB L 174 van 1.7.2011, blz. 1).

⁽⁷⁾ Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

⁽⁸⁾ Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 82/891/EEG van de Raad en de Richtlijnen 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU en 2013/36/EU en de Verordeningen (EU) nr. 1093/2010 en (EU) nr. 648/2012, van het Europees Parlement en de Raad (PB L 173 van 12.6.2014, blz. 190).

⁽⁹⁾ Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

⁽¹⁰⁾ Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).

⁽¹¹⁾ Richtlijn (EU) 2016/2341 van het Europees Parlement en de Raad van 14 december 2016 betreffende de werkzaamheden van en het toezicht op instellingen voor bedrijfspensioenvoorziening (IBPV's) (PB L 354 van 23.12.2016, blz. 37).

⁽¹²⁾ Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (zie bladzijde 1 van dit Publicatieblad).

⁽¹³⁾ Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

kader voor digitale operationele weerbaarheid, moet het toepassingsgebied van de SREP ook worden gewijzigd opdat expliciet naar de vereisten van Verordening (EU) 2022/2554 wordt verwezen en met name de risico's worden bestreken die aan het licht zijn gekomen dankzij verslagen over ernstige ICT-gerelateerde incidenten en dankzij de resultaten van de tests inzake digitale operationele weerbaarheid die financiële entiteiten overeenkomstig die verordening uitvoeren.

- (5) Digitale operationele weerbaarheid is essentieel om de kritieke functies en de centrale bedrijfsonderdelen van een financiële entiteit in geval van afwikkeling te behouden en zo een verstoring van de reële economie en het financiële stelsel te voorkomen. Ernstige operationele incidenten kunnen een belemmering vormen voor het vermogen van een financiële entiteit om haar activiteiten voort te zetten en kunnen de afwikkelingsdoelstellingen in gevaar brengen. Bepaalde contractuele overeenkomsten inzake het gebruik van ICT-diensten zijn van essentieel belang om de operationele continuïteit te waarborgen en in geval van afwikkeling de nodige gegevens te verstrekken. Om afgestemd te zijn op de doelstellingen van het Uniekader voor operationele weerbaarheid moet Richtlijn 2014/59/EU dienovereenkomstig worden gewijzigd, om ervoor te zorgen dat bij de afwikkelingsplanning en de beoordeling van de afwikkelbaarheid van financiële entiteiten rekening wordt gehouden met de informatie in verband met operationele weerbaarheid.
- (6) Richtlijn 2014/65/EU voorziet in strengere ICT-risicovoorschriften voor beleggingsondernemingen en handelsplatformen die zich bezighouden met algoritmische handel. Voor datarapporteringsdiensten en transactieregisters gelden minder gedetailleerde vereisten. Ook bevat Richtlijn 2014/65/EU slechts beperkte verwijzingen naar controle- en beveiligingsregelingen voor informatieverwerkingssystemen en naar het gebruik van passende systemen, middelen en procedures om de continuïteit en regelmatigheid van de zakelijke diensten te waarborgen. Voorts moet die richtlijn worden afgestemd op Verordening (EU) 2022/2554 wat betreft continuïteit en regelmatigheid bij de verrichting van beleggingsdiensten en -activiteiten, operationele weerbaarheid, de capaciteit van handelssystemen en de doeltreffendheid van bedrijfscontinuïteitsregelingen en risicobeheer.
- (7) Richtlijn (EU) 2015/2366 bevat specifieke regels inzake ICT-beveiligingscontroles en risicobeperking met het oog op het verkrijgen van een machtiging tot het verrichten van betalingsdiensten. Deze machtigingsregels moeten worden gewijzigd om ze in overeenstemming te brengen met Verordening (EU) 2022/2554. Om de administratieve lasten te verminderen en complexe en overlappende rapportagevereisten te vermijden mogen daarnaast de in die richtlijn vervatte regels voor incidentenmelding niet langer van toepassing zijn op betalingsdienstaanbieders die onder die richtlijn en tevens onder Verordening (EU) 2022/2554 vallen, zodat die betalingsdienstaanbieders kunnen profiteren van één volledig geharmoniseerd mechanisme voor de melding van alle betalingsgerelateerde operationele of beveiligingsincidenten, ongeacht of dergelijke incidenten ICT-gerelateerd zijn.
- (8) In de algemene bepalingen over governance en risicobeheer van Richtlijn 2009/138/EG en Richtlijn (EU) 2016/2341 komt het ICT-risico gedeeltelijk aan bod; bepaalde vereisten moeten worden gespecificeerd door middel van gedelegeerde handelingen met of zonder specifieke verwijzingen naar het ICT-risico. Ook voor beheerders van alternatieve beleggingsfondsen die onder Richtlijn 2011/61/EU en beheersmaatschappijen die onder Richtlijn 2009/65/EG vallen, gelden slechts zeer algemene regels. Die richtlijnen moeten dus worden afgestemd op de vereisten van Verordening (EU) 2022/2554 wat betreft het beheer van ICT-systemen en -instrumenten.
- (9) In heel wat gevallen zijn in gedelegeerde en uitvoeringshandelingen al verdere ICT-risicovereisten vastgelegd op basis van ontwerpen van technische reguleringsnormen en ontwerpen van technische uitvoeringsnormen die door de bevoegde Europese toezichthoudende autoriteit zijn ontwikkeld. Aangezien de bepalingen van Verordening (EU) 2022/2554 voortaan het rechtskader vormen voor het ICT-risico in de financiële sector, moeten bepaalde machtigingen om gedelegeerde handelingen en uitvoeringshandelingen vast te stellen in de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU en 2014/65/EU worden gewijzigd om de ICT-risicobepalingen uit het toepassingsgebied van die machtigingen te halen.
- (10) Om te zorgen voor de consistente toepassing van het nieuwe kader voor digitale operationele weerbaarheid in de financiële sector, moeten de lidstaten de bepalingen van nationaal recht tot omzetting van deze richtlijn toepassen vanaf de datum van toepassing van Verordening (EU) 2022/2554.

- (11) De Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 zijn vastgesteld op basis van artikel 53, lid 1, of artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), of beide. De wijzigingen in deze richtlijn zijn in één wetgevingshandeling opgenomen vanwege de verwevenheid van het onderwerp en de doelstellingen van de wijzigingen. Bijgevolg moet deze richtlijn worden vastgesteld op basis van zowel artikel 53, lid 1, als artikel 114 VWEU.
- (12) Daar de doelstellingen van deze richtlijn niet voldoende door de lidstaten kunnen worden verwezenlijkt omdat zij een harmonisatie inhouden van voorschriften die reeds in richtlijnen vervat zijn, maar vanwege de omvang en de gevolgen van het optreden beter door de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om die doelstellingen te verwezenlijken.
- (13) Overeenkomstig de gezamenlijke politieke verklaring van 28 september 2011 van de lidstaten en de Commissie over toelichtende stukken ⁽¹⁴⁾ hebben de lidstaten zich ertoe verbonden om in gerechtvaardigde gevallen de kennisgeving van hun omzettingsmaatregelen vergezeld te doen gaan van één of meer stukken waarin het verband tussen de onderdelen van een richtlijn en de overeenkomstige delen van de nationale omzettinginstrumenten wordt toegelicht. Met betrekking tot deze richtlijn acht de wetgever de toezending van die stukken gerechtvaardigd,

HEBBER DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1

Wijzigingen in Richtlijn 2009/65/EG

Artikel 12 van Richtlijn 2009/65/EG wordt als volgt gewijzigd:

1) In lid 1, tweede alinea, wordt punt a) vervangen door:

- “a) moet beschikken over een goede administratieve en boekhoudkundige organisatie, controle- en beveiligingsvoorzieningen op het gebied van elektronische informatieverwerking, onder meer wat betreft netwerk- en informatiesystemen die worden opgericht en beheerd overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*), evenals over adequate interne controleprocedures, met inbegrip van met name regels voor persoonlijke transacties van de eigen medewerkers en voor het aanhouden of beheren van beleggingen in financiële instrumenten met het oog op het beleggen voor eigen rekening, die ten minste waarborgen dat elke transactie waarbij de icbe betrokken is, kan worden gereconstrueerd wat betreft de oorsprong ervan, de betrokken partijen, de aard ervan, en de tijd en de plaats waar zij heeft plaatsgevonden, en dat de activa van de door de beheermaatschappij beheerde icbe, overeenkomstig het fondsreglement of de statuten en de vigerende wettelijke bepalingen worden belegd;

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”

2) Lid 3 wordt vervangen door:

“3. Onverminderd de bepalingen van artikel 116 stelt de Commissie middels gedelegeerde handelingen overeenkomstig artikel 112 bis maatregelen vast ter nadere bepaling van:

- a) de procedures en regelingen als bedoeld in lid 1, tweede alinea, punt a), voor zover zij geen betrekking hebben op de procedures en regelingen inzake netwerk- en informatiesystemen;
- b) de structuren en organisatorische eisen ter beperking van belangenconflicten als bedoeld in lid 1, tweede alinea, punt b).”

⁽¹⁴⁾ PB C 369 van 17.12.2011, blz. 14.

*Artikel 2***Wijzigingen in Richtlijn 2009/138/EG**

Richtlijn 2009/138/EG wordt als volgt gewijzigd:

1) In artikel 41 wordt lid 4 vervangen door:

“4. Verzekerings- en herverzekeringsondernemingen treffen redelijke maatregelen, waaronder de ontwikkeling van noodplannen, om voor continuïteit en regelmatigheid in de verrichting van hun werkzaamheden te zorgen. Te dien einde worden door de ondernemingen passende en evenredige systemen, middelen en procedures gebruikt, en met name netwerk- en informatiesystemen gecreëerd en beheerd overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*).

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”

2) In artikel 50, lid 1, worden de punten a) en b) vervangen door:

“a) de onderdelen van de in artikel 41, artikel 44, met name op de in artikel 44, lid 2, genoemde gebieden, en de artikelen 46 en 47 bedoelde systemen, voor zover zij geen betrekking hebben op het beheer van informatie- en communicatietechnologierisico's;

b) de in de artikelen 44, 46, 47 en 48 bedoelde functies, voor zover het niet gaat om functies die verband houden met het beheer van informatie- en communicatietechnologierisico's.”

*Artikel 3***Wijzigingen in Richtlijn 2011/61/EU**

Artikel 18 van Richtlijn 2011/61/EU wordt vervangen door:

“Artikel 18

Algemene beginselen

1. De lidstaten eisen dat abi-beheerders te allen tijde over adequate en voldoende personele en technische middelen beschikken om het beheer van abi's naar behoren te kunnen uitvoeren.

Mede in het licht van de aard van het door de abi-beheerder beheerde abi schrijven de bevoegde autoriteiten van de lidstaat van herkomst met name voor dat de abi-beheerder moet beschikken over goede administratieve en boekhoudkundige procedures, controle- en beveiligingsvoorschriften voor elektronische gegevensverwerking, onder meer met betrekking tot netwerk- en informatiesystemen die worden opgericht en beheerd overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*), evenals adequate interne controleprocedures, met inbegrip van met name regels voor persoonlijke transacties van de eigen medewerkers en voor het aanhouden of beheren van beleggingen met het oog op het beleggen van het eigen vermogen, zodat op zijn minst gewaarborgd wordt dat elke transactie waarbij de abi's betrokken zijn, kan worden gereconstrueerd wat betreft de oorsprong ervan, de erbij betrokken partijen, de aard ervan en de tijd en de plaats waar de transactie heeft plaatsgevonden, en dat de activa van de door de abi-beheerder beheerde abi worden belegd in overeenstemming met het reglement van de abi of de statuten en de vigerende wettelijke bepalingen.

2. De Commissie stelt middels gedelegeerde handelingen overeenkomstig artikel 56 en onder de voorwaarden van de artikelen 57 en 58 maatregelen vast tot precisering van de procedures en regels waarvan sprake is in lid 1 van dit artikel, voor zover zij geen betrekking hebben op de procedures en regelingen inzake netwerk- en informatiesystemen.

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27 12.2022, blz. 1).”

Artikel 4

Wijzigingen in Richtlijn 2013/36/EU

Richtlijn 2013/36/EU wordt als volgt gewijzigd:

1) In artikel 65, lid 3, wordt punt a), vi), vervangen door:

“vi) derden aan wie de in de punten i) tot en met iv) bedoelde entiteiten functies of activiteiten hebben uitbesteed, met inbegrip van derde aanbieders van ICT-diensten, zoals bedoeld in hoofdstuk V van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*);

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”.

2) In artikel 74, lid 1, wordt de eerste alinea vervangen door:

“De instellingen beschikken over solide governanceregelingen, waaronder een duidelijke organisatiestructuur met duidelijk omschreven, transparante en samenhangende verantwoordelijkheden, effectieve procedures voor het identificeren, het beheer, de bewaking en de rapportage van de risico's waaraan zij blootstaan of bloot kunnen komen te staan, adequate internecontrolemechanismen, zoals degelijke administratieve en boekhoudkundige procedures, netwerk- en informatiesystemen die overeenkomstig Verordening (EU) 2022/2554 worden opgericht en beheerd, en een beloningsbeleid en een beloningspraktijk die in overeenstemming zijn met en bijdragen tot een degelijk en doeltreffend risicobeheer.”.

3) In artikel 85 wordt lid 2 vervangen door:

“2. De bevoegde autoriteiten zorgen ervoor dat de instellingen over gepaste nood- en bedrijfscontinuïteitsbeleidslijnen en -plannen beschikken, inclusief beleidslijnen en plannen inzake ICT-bedrijfscontinuïteit en respons- en herstelplannen voor ICT wat betreft de technologie die zij gebruiken om informatie te verstrekken, en dat die plannen worden opgesteld, beheerd en getest overeenkomstig artikel 11 van Verordening (EU) 2022/2554, teneinde instellingen in staat te stellen hun activiteiten voort te zetten in geval van een ernstige verstoring van de bedrijfsactiviteiten en de verliezen als gevolg van een dergelijke verstoring te beperken.”.

4) In artikel 97, lid 1, wordt het volgende punt toegevoegd:

“d) risico's die aan het licht zijn gekomen bij tests inzake de digitale operationele weerbaarheid overeenkomstig hoofdstuk IV van Verordening (EU) 2022/2554.”.

Artikel 5

Wijzigingen in Richtlijn 2014/59/EU

Richtlijn 2014/59/EU wordt als volgt gewijzigd:

1) Artikel 10 wordt als volgt gewijzigd:

a) in lid 7 wordt punt c) vervangen door:

“c) een demonstratie van de wijze waarop de kritieke functies en de kernbedrijfsonderdelen juridisch en economisch voldoende van de overige functies kunnen worden gescheiden om bij falen van de instelling de continuïteit en digitale operationele weerbaarheid te waarborgen;”;

b) in lid 7 wordt punt q) vervangen door:

“q) een beschrijving van de verrichtingen en systemen die essentieel zijn voor het behoud van de continuïteit van de operationele processen van de instelling, met inbegrip van netwerk- en informatiesystemen als bedoeld in Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*);

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”;

c) aan lid 9 wordt de volgende alinea toegevoegd:

“In overeenstemming met artikel 10 van Verordening (EU) nr. 1093/2010 evalueert en, in voorkomend geval, actualiseert de EBA de technische reguleringsnormen om onder meer rekening te houden met de bepalingen van hoofdstuk II van Verordening (EU) 2022/2554.”.

2) De bijlage wordt als volgt gewijzigd:

a) in deel A wordt punt 16) vervangen door:

“16) de regelingen en maatregelen die nodig zijn voor het behoud van de continuïteit van de operationele processen van de instelling, met inbegrip van de netwerk- en informatiesystemen die zijn opgericht en worden beheerd overeenkomstig Verordening (EU) 2022/2554;”;

b) deel B wordt als volgt gewijzigd:

i) punt 14) wordt vervangen door:

“14) de identificatie van de eigenaars van de in punt 13) genoemde systemen, de daarmee verband houdende dienstenniveauovereenkomsten en eventuele software en systemen of licenties, met een uitsplitsing naar hun rechtspersonen, kritieke bedrijfsactiviteiten en kernbedrijfsonderdelen, evenals de identificatie van kritieke externe aanbieders van ICT-diensten zoals gedefinieerd in artikel 3, punt 23, van Verordening (EU) 2022/2554;”;

ii) het volgende punt wordt toegevoegd:

“14 bis) de resultaten van de tests van instellingen inzake digitale operationele weerbaarheid uit hoofde van Verordening (EU) 2022/2554;”;

c) deel C wordt als volgt gewijzigd:

i) punt 4 wordt vervangen door:

“4. de mate waarin de dienstverleningsovereenkomsten waarover de instelling beschikt, met inbegrip van de contractuele overeenkomsten inzake het gebruik van ICT-diensten, robuust en volledig afdwingbaar zijn in geval van de afwikkeling van de instelling;”;

ii) het volgende punt wordt ingevoegd:

“4 bis. de digitale operationele weerbaarheid van de netwerk- en informatiesystemen die kritieke functies en kernbedrijfsonderdelen van de instelling ondersteunen, rekening houdend met verslagen over ernstige ICT-gerelateerde incidenten en de resultaten van tests van digitale operationele weerbaarheid uit hoofde van Verordening (EU) 2022/2554;”.

Artikel 6

Wijzigingen in Richtlijn 2014/65/EU

Richtlijn 2014/65/EU wordt als volgt gewijzigd:

1) Artikel 16 wordt als volgt gewijzigd:

a) lid 4 wordt vervangen door:

“4. Een beleggingsonderneming treft redelijke maatregelen om continuïteit en regelmatigheid bij het verlenen van beleggingsdiensten en het verrichten van beleggingsactiviteiten te waarborgen. Te dien einde maakt de beleggingsonderneming gebruik van passende en evenredige systemen, met inbegrip van ICT-systemen die zijn opgericht en worden beheerd overeenkomstig artikel 7 van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*), evenals van passende en evenredige middelen en procedures.

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”;

- b) in lid 5 worden de tweede en derde alinea vervangen door:

“Een beleggingsonderneming beschikt over een goede administratieve en boekhoudkundige organisatie, adequate interne controlemechanismen en effectieve risicobeoordelingsprocedures.

Onverminderd de mogelijkheid voor de bevoegde autoriteiten om toegang tot communicatie te vragen overeenkomstig deze richtlijn en Verordening (EU) nr. 600/2014 beschikt een beleggingsonderneming over deugdelijke beveiligingsmechanismen om, overeenkomstig de vereisten van Verordening (EU) 2022/2554 de beveiliging en authenticatie van de middelen voor de informatieoverdracht te waarborgen, het risico op datacorruptie en ongeoorloofde toegang tot een minimum te beperken en te voorkomen dat informatie uitlekt door de vertrouwelijkheid van de gegevens te allen tijde te bewaren.”.

- 2) Artikel 17 wordt als volgt gewijzigd:

- a) lid 1 wordt vervangen door:

“1. Een beleggingsonderneming die zich met algoritmische handel bezighoudt, heeft voor haar bedrijfsactiviteit geschikte, doeltreffende systemen en risicocontroles ingesteld om te garanderen dat haar handelssystemen weerbaar zijn en voldoende capaciteit hebben overeenkomstig de vereisten van hoofdstuk II van Verordening (EU) 2022/2554, aan gepaste handelsdrempels en -limieten onderworpen zijn, en te voorkomen dat foutieve orders worden verzonden of dat de systemen anderszins op zodanige wijze functioneren dat zulks tot het ontstaan van een onordelijke markt kan leiden of bijdragen.

Een dergelijke onderneming heeft ook doeltreffende systemen en risicocontroles ingesteld om te garanderen dat de handelssystemen niet kunnen worden aangewend voor enigerlei doel dat in strijd is met Verordening (EU) nr. 596/2014 of met de regels van een handelsplatform waarmee zij is verbonden.

De beleggingsonderneming beschikt over doeltreffende regelingen om de bedrijfscontinuïteit bij elke storing van haar handelssystemen te garanderen, met inbegrip van overeenkomstig artikel 11 van Verordening (EU) 2022/2554 opgestelde beleidslijnen en plannen inzake ICT-bedrijfscontinuïteit en respons- en herstelplannen voor ICT, en ziet erop toe dat haar systemen volledig zijn getest en naar behoren worden gecontroleerd om te garanderen dat zij aan de algemene vereisten van dit lid en aan de specifieke vereisten van de hoofdstukken II en IV van Verordening (EU) 2022/2554 voldoen.”;

- b) in lid 7 wordt punt a) vervangen door:

“a) gedetailleerde informatie inzake de in de leden 1 tot en met 6 gestelde organisatorische eisen die geen betrekking hebben op ICT-risicobeheer en die moeten worden opgelegd aan beleggingsondernemingen die verschillende beleggingsdiensten, beleggingsactiviteiten, nevendiensten of combinaties daarvan verlenen of verrichten. In de gedetailleerde informatie inzake de in lid 5 gestelde organisatorische eisen worden de specifieke vereisten voor directe markttoegang en voor gesponsorde toegang vastgelegd op een wijze die garandeert dat de voor gesponsorde toegang toegepaste controles ten minste gelijkwaardig zijn aan de voor directe markttoegang toegepaste controles;”.

- 3) In artikel 47 wordt lid 1 als volgt gewijzigd:

- a) punt b) wordt vervangen door:

“b) adequaat toegerust is voor het beheer van de risico's waaraan zij blootgesteld is, met inbegrip van het beheer van het ICT-risico overeenkomstig hoofdstuk II van Verordening (EU) 2022/2554, in passende regelingen en systemen voorziet om risico's van betekenis voor de exploitatie te onderkennen, en doeltreffende maatregelen treft om deze risico's te beperken;”;

- b) punt c) wordt geschrapt;

- 4) Artikel 48 wordt als volgt gewijzigd:

- a) lid 1 wordt vervangen door:

“1. De lidstaten schrijven voor dat een gereguleerde markt zijn operationele weerbaarheid moet opbouwen en onderhouden in overeenstemming met de vereisten in hoofdstuk II van Verordening (EU) 2022/2554 om te waarborgen dat zijn handelssystemen weerbaar zijn, voldoende capaciteit hebben om volumepeiken in orders en orderberichten op te vangen, in staat zijn een ordelijke handel onder zeer gespannen marktomstandigheden te waarborgen, volledig zijn getest om te garanderen dat aan deze voorwaarden is voldaan, en onderworpen zijn aan doeltreffende regelingen ter verzekering van de continuïteit van de bedrijfsuitoefening, inclusief beleidslijnen en plannen inzake ICT-bedrijfscontinuïteit en respons- en herstelplannen voor ICT overeenkomstig artikel 11 van Verordening (EU) 2022/2554, teneinde de continuïteit van de dienstverlening te verzekeren in geval van een storing van zijn handelssystemen.”;

b) lid 6 wordt vervangen door:

“6. De lidstaten schrijven voor dat een gereglementeerde markt voorziet in doeltreffende systemen, procedures en regelingen, inclusief de verplichting voor leden of deelnemers om algoritmen adequaat te testen en omgevingen te bieden om deze tests te faciliteren overeenkomstig de vereisten van de hoofdstukken II en IV van Verordening (EU) 2022/2554, om te voorkomen dat systemen voor algoritmische handel tot het ontstaan van onordelijke handelsomstandigheden op de markt kunnen leiden of bijdragen en om alle onordelijke handelsomstandigheden die door deze systemen voor algoritmische handel ontstaan, te beheren, met inbegrip van systemen om de verhouding tussen het aantal niet-uitgevoerde orders en het aantal transacties dat door een lid of deelnemer in het handelssysteem kan worden ingevoerd te beperken, om in staat te zijn de orderstroom af te remmen indien het risico bestaat dat de systeemcapaciteit wordt bereikt, en om de minimale verhandelingsseenheid op de markt te beperken en te handhaven.”;

c) lid 12 wordt als volgt gewijzigd:

i) punt a) wordt vervangen door:

“a) de vereisten om te waarborgen dat de handelssystemen van gereglementeerde markten weerbaar zijn en voldoende capaciteit hebben, met uitzondering van de vereisten in verband met de digitale operationele weerbaarheid;”;

ii) punt g) wordt vervangen door:

“g) de vereisten om ervoor te zorgen dat algoritmen adequaat worden getest — behalve wat hun digitale operationele weerbaarheid betreft — om te voorkomen dat systemen voor algoritmische handel met inbegrip van hoogfrequentie algoritmische handel kunnen leiden of bijdragen tot het ontstaan van onordelijke handelsomstandigheden op de markt.”.

Artikel 7

Wijzigingen in Richtlijn (EU) 2015/2366

Richtlijn (EU) 2015/2366 wordt als volgt gewijzigd:

1) In artikel 3 wordt punt j) vervangen door:

“j) door technischediensaanbieders verrichte diensten ter ondersteuning van het aanbieden van betalingsdiensten, waarbij de betrokken aanbieders op geen enkel moment in het bezit komen van de over te maken geldmiddelen, met inbegrip van verwerking en opslag van gegevens, diensten ter bescherming van het vertrouwen en het privéleven, authenticatie van gegevens en entiteiten, levering van informatie- en communicatietechnologie (ICT) en van communicatienetwerken, alsmede levering en onderhoud van voor betalingsdiensten gebruikte automaten en instrumenten, met uitzondering van betalingsinitiatiediensten en rekeninginformatiediensten;”.

2) Artikel 5, lid 1, wordt als volgt gewijzigd:

a) de eerste alinea wordt als volgt gewijzigd:

i) punt e) wordt vervangen door:

“e) een beschrijving van de regelingen op het gebied van bestuur (governance) en de mechanismen voor interne controle die de aanvrager heeft ingesteld, waaronder de administratieve en boekhoudkundige procedures en de procedures voor risicobeheer, alsook de regelingen voor het gebruik van ICT-diensten overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*), waaruit blijkt dat die bestuursregelingen en interne controlemechanismen evenredig, passend, degelijk en adequaat zijn;

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”;

ii) punt f) wordt vervangen door:

“f) een beschrijving van de procedures voor het monitoren en afhandelen van veiligheidsincidenten en veiligheidsgerelateerde klachten van cliënten en voor de follow-up ervan, met inbegrip van een mechanisme voor het melden van incidenten dat rekening houdt met de kennisgevingsverplichtingen voor betalingsinstellingen die zijn vastgelegd in hoofdstuk III van Verordening (EU) 2022/2554;”;

iii) punt h) wordt vervangen door:

“h) een beschrijving van de bedrijfscontinuïteitsregelingen, met daarin een duidelijke uiteenzetting van de kritieke bedrijfsactiviteiten, alsmede doeltreffende beleidslijnen en plannen inzake ICT-bedrijfscontinuïteit en respons- en herstelplannen voor ICT en een procedure om de toereikendheid en efficiëntie van deze plannen regelmatig te beproeven en te herzien overeenkomstig Verordening (EU) 2022/2554;”

b) de derde alinea wordt vervangen door:

“Bij de in punt j) van de eerste alinea bedoelde maatregelen op het gebied van beveiligingscontrole en risicobeperking wordt aangegeven op welke wijze een hoog niveau van digitale operationele weerbaarheid wordt gewaarborgd overeenkomstig hoofdstuk II van Verordening (EU) 2022/2554, met name wat betreft technische beveiliging en gegevensbescherming, ook wat betreft de software en ICT-systemen die worden gebruikt door de aanvrager of door ondernemingen waaraan de aanvrager zijn activiteiten geheel of gedeeltelijk uitbesteedt. Deze maatregelen omvatten tevens de bij artikel 95, lid 1, van deze richtlijn vastgestelde beveiligingsmaatregelen. Bij het opstellen van deze maatregelen wordt tevens rekening gehouden met de in artikel 95, lid 3, van deze richtlijn bedoelde EBA-richtsnoeren inzake beveiligingsmaatregelen, zodra die zijn vastgesteld.”

3) In artikel 19, lid 6, wordt de tweede alinea vervangen door:

“Bij het uitbesteden van belangrijke operationele taken, waaronder ICT-systemen, mag niet wezenlijk afbreuk worden gedaan aan de kwaliteit van de interne controle van de betalingsinstelling, noch aan het vermogen van de bevoegde autoriteiten om te controleren en na te gaan of de betalingsinstelling alle in deze richtlijn neergelegde verplichtingen nakomt.”

4) Aan artikel 95, lid 1, wordt de volgende alinea toegevoegd:

“De eerste alinea doet geen afbreuk aan de toepassing van hoofdstuk II van Verordening (EU) 2022/2554 op:

- a) betalingsdienstaanbieders als bedoeld in artikel 1, lid 1, punten a), b) en d), van deze richtlijn;
- b) aanbieders van rekeninginformatiediensten als bedoeld in artikel 33, lid 1, van deze richtlijn;
- c) uit hoofde van artikel 32, lid 1, van deze richtlijn vrijgestelde betalingsinstellingen; en
- d) instellingen voor elektronisch geld waaraan een ontheffing is verleend als bedoeld in artikel 9, lid 1, van Richtlijn 2009/110/EG.”

5) Aan artikel 96 wordt het volgende lid toegevoegd:

“7. De lidstaten zorgen ervoor dat de leden 1 tot en met 5 van dit artikel niet van toepassing zijn op:

- a) betalingsdienstaanbieders als bedoeld in artikel 1, lid 1, punten a), b) en d), van deze richtlijn;
- b) aanbieders van rekeninginformatiediensten als bedoeld in artikel 33, lid 1, van deze richtlijn;
- c) uit hoofde van artikel 32, lid 1, van deze richtlijn vrijgestelde betalingsinstellingen;
- d) instellingen voor elektronisch geld waaraan een ontheffing is verleend als bedoeld in artikel 9, lid 1, van Richtlijn 2009/110/EG.”

6) In artikel 98 wordt lid 5 vervangen door:

“5. In overeenstemming met artikel 10 van Verordening (EU) nr. 1093/2010 evalueert en, in voorkomend geval, actualiseert EBA de technische reguleringsnormen regelmatig om onder meer rekening te houden met innovatie en technologische ontwikkelingen en met de bepalingen van hoofdstuk II van Verordening (EU) 2022/2554.”

Artikel 8

Wijziging in Richtlijn (EU) 2016/2341

Artikel 21, lid 5, van Richtlijn (EU) 2016/2341 wordt vervangen door:

“5. De lidstaten zorgen ervoor dat IBPV's redelijke maatregelen treffen, waaronder de ontwikkeling van noodplannen, om voor continuïteit en regelmatigheid in de verrichting van hun werkzaamheden te zorgen. Te dien

einde worden door IBPV's passende en evenredige systemen, middelen en procedures gebruikt en, indien nodig, met name netwerk- en informatiesystemen gecreëerd en beheerd overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*).

(*) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).”.

Artikel 9

Omzetting

1. De lidstaten dienen uiterlijk op 17 januari 2025 de bepalingen vast te stellen en bekend te maken die nodig zijn om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onmiddellijk in kennis.

Zij passen die bepalingen toe met ingang van 17 januari 2025.

Wanneer de lidstaten die bepalingen aannemen, wordt in die bepalingen zelf of bij de officiële bekendmaking ervan naar deze richtlijn verwezen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten delen de Commissie de tekst van de belangrijkste bepalingen van intern recht mede die zij op het onder deze richtlijn vallende gebied vaststellen.

Artikel 10

Inwerkingtreding

Deze richtlijn treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Artikel 11

Adressaten

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Straatsburg, 14 december 2022.

Voor het Europees Parlement
De voorzitter
R. METSOLA

Voor de Raad
De voorzitter
M. BEK