DIRECTIVE (EU) 2022/2556 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 53(1) and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The Union needs to adequately and comprehensively address digital risks to all financial entities stemming from an increased use of information and communication technology (ICT) in the provision and consumption of financial services, thereby contributing to the realisation of the potential of digital finance, in terms of boosting innovation and promoting competition in a secure digital environment.

(2) Financial entities are heavily reliant on the use of digital technologies in their daily business. It is therefore of utmost importance to ensure the operational resilience of their digital operations against ICT risk. This need has become even more pressing due to the growth of breakthrough technologies in the market, in particular technologies enabling digital representations of value or of rights to be transferred and stored electronically, using distributed ledger or similar technology (crypto-assets), and of services related to those assets.

([1]) OJ C 343, 26.8.2021, p. 1.
([2]) OJ C 155, 30.4.2021, p. 38.
([3]) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

(3) At Union level, the requirements related to the management of ICT risk in the financial sector are currently provided for in Directives 2009/65/EC ([4]), 2009/138/EC ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) and (EU) 2016/2341 ([11]) of the European Parliament and of the Council.

Those requirements are diverse and occasionally incomplete. In some cases, ICT risk has been addressed only implicitly as part of operational risk, and in other cases it has not been addressed at all. Those issues are remedied by the adoption of Regulation (EU) 2022/2554 of the European Parliament and of the Council ([12]). Those Directives should therefore be amended to ensure consistency with that Regulation. This Directive enacts a set of amendments that are necessary to bring legal clarity and consistency in relation to the application, by financial entities authorised and supervised in accordance with those Directives, of various digital operational resilience requirements that are necessary in the pursuit of their activities and in the provision of services, thereby guaranteeing the smooth functioning of the internal market. It is necessary to ensure the adequacy of those requirements in relation to market developments, while encouraging proportionality in particular with regard to the size of financial entities and the specific regimes to which they are subject, with the aim of reducing compliance costs.

(4) In the area of banking services, Directive 2013/36/EU currently sets out only general internal governance rules and operational risk provisions containing requirements for contingency and business continuity plans which implicitly serve as a basis for addressing ICT risk. However, in order to address ICT risk explicitly and clearly, the requirements for contingency and business continuity plans should be amended to also include business continuity plans and response and recovery plans concerning ICT risk, in accordance with the requirements laid down in Regulation (EU) 2022/2554. Furthermore, ICT risk is only implicitly included, as part of operational risk, in the supervisory review and evaluation process (SREP) performed by competent authorities and the criteria for its assessment are currently defined in the Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP), issued by the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([13]). In order to provide legal clarity and ensure that bank supervisors effectively identify ICT risk, and monitor its management by financial entities, in

([4]) Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (OJ L 302, 17.11.2009, p. 32).

([5]) Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

([6]) Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

([7]) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

([8]) Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

([9]) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

([10]) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

([11]) Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).

([12]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (See page1 of this Official Journal).

([13]) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

line with the new framework on digital operational resilience, the scope of the SREP should also be amended to explicitly refer to the requirements laid down in Regulation (EU) 2022/2554 and to cover in particular the risks revealed by major ICT-related incident reports and by the results of the digital operational resilience testing performed by financial entities in accordance with that Regulation.

(5) Digital operational resilience is essential to preserve the critical functions and core business lines of a financial entity in the event of its resolution, and thereby to avoid disruption to the real economy and to the financial system. Major operational incidents can hamper the capacity of a financial entity to continue operating and can jeopardise resolution objectives. Certain contractual arrangements on the use of ICT services are essential to ensure operational continuity and to provide the necessary data in the event of resolution. In order to be aligned with the objectives of the Union framework for operational resilience, Directive 2014/59/EU should be amended accordingly, with a view to ensuring that information relating to operational resilience is taken into account in the context of resolution planning and the assessment of financial entities' resolvability.

(6) Directive 2014/65/EU sets out more stringent ICT risk rules for investment firms and trading venues that are engaging in algorithmic trading. Less detailed requirements apply to data reporting services and to trade repositories. Also, Directive 2014/65/EU contains only limited references to control and safeguard arrangements for information processing systems and to the use of appropriate systems, resources and procedures to ensure continuity and regularity of business services. Furthermore, that Directive should be aligned with Regulation (EU) 2022/2554 as regards continuity and regularity in the provision of investment services and in the performance of investment activities, operational resilience, the capacity of trading systems, and the effectiveness of business continuity arrangements and risk management.

(7) Directive (EU) 2015/2366 sets out specific rules on ICT security controls and mitigation elements for the purposes of obtaining an authorisation to provide payment services. Those authorisation rules should be amended to align them with Regulation (EU) 2022/2554. Furthermore, in order to reduce the administrative burden and to avoid complexity and duplicative reporting requirements, the incident reporting rules in that Directive should cease to apply to payment service providers which are regulated under that Directive and also subject to Regulation (EU) 2022/2554, thus allowing those payment service providers to benefit from a single, fully harmonised incident reporting mechanism with regard to all operational or security payment-related incidents, irrespective of whether such incidents are ICT-related.

(8) Directives 2009/138/EC and (EU) 2016/2341 partially capture ICT risk within their general provisions on governance and risk management, leaving certain requirements to be specified through delegated acts with or without specific references to ICT risk. Similarly, only very general rules apply to managers of alternative investment funds subject to Directive 2011/61/EU and management companies subject to Directive 2009/65/EC. Those Directives should therefore be aligned with the requirements laid down in Regulation (EU) 2022/2554 with regard to the management of ICT systems and tools.

(9) In many cases, further ICT risk requirements have already been laid down in delegated and implementing acts, adopted on the basis of draft regulatory technical standards and draft implementing technical standards developed by the competent European Supervisory Authority. Since the provisions of Regulation (EU) 2022/2554 henceforth constitute the legal framework for ICT risk in the financial sector, certain empowerments to adopt delegated and implementing acts in Directives 2009/65/EC, 2009/138/EC, 2011/61/EU and 2014/65/EU should be amended to remove the ICT risk provisions from the scope of those empowerments.

(10) To ensure a consistent implementation of the new framework on digital operational resilience for the financial sector, Member States should apply the provisions of national law transposing this Directive from the date of application of Regulation (EU) 2022/2554.

(11) Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 have been adopted on the basis of Article 53(1) or Article 114 of the Treaty on the Functioning of the European Union (TFEU) or both. The amendments in this Directive have been included in a single legislative act due to the interconnectedness of the subject matter and objectives of the amendments. Consequently, this Directive should be adopted on the basis of both Article 53(1) and Article 114 TFEU.

(12) Since the objectives of this Directive cannot be sufficiently achieved by the Member States as they entail the harmonisation of requirements already contained in Directives but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(13) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([14]), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Amendments to Directive 2009/65/EC

Article 12 of Directive 2009/65/EC is amended as follows:

(1) in the second subparagraph of paragraph 1, point (a) is replaced by the following:

'(a) has sound administrative and accounting procedures, control and safeguard arrangements for electronic data processing, including with regard to network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as adequate internal control mechanisms, including, in particular, rules for personal transactions by its employees or for the holding or management of investments in financial instruments in order to invest on its own account and ensuring, at least, that each transaction involving the UCITS may be reconstructed according to its origin, the parties to it, its nature, and the time and place at which it was effected and that the assets of the UCITS managed by the management company are invested according to the fund rules or the instruments of incorporation and the legal provisions in force;

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) paragraph 3 is replaced by the following:

'3. Without prejudice to Article 116, the Commission shall adopt, by means of delegated acts in accordance with Article 112a, measures specifying:

(a) the procedures and arrangements referred to in point (a) of the second subparagraph of paragraph 1, other than the procedures and arrangements concerning network and information systems;

(b) the structures and organisational requirements to minimise conflicts of interests referred to in point (b) of the second subparagraph of paragraph 1.'.

([14]) OJ C 369, 17.12.2011, p. 14.

Article 2

Amendments to Directive 2009/138/EC

Directive 2009/138/EC is amended as follows:

(1) in Article 41, paragraph 4 is replaced by the following:

'4. Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertakings shall employ appropriate and proportionate systems, resources and procedures, and shall, in particular, set up and manage network and information systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) in Article 50(1), points (a) and (b) are replaced by the following:

'(a) the elements of the systems referred to in Article 41, Article 44, in particular the areas listed in Article 44(2), and Articles 46 and 47, other than the elements concerning information and communication technology risk management;

(b) the functions referred to in Articles 44, 46, 47 and 48, other than functions related to information and communication technology risk management.'.

Article 3

Amendment to Directive 2011/61/EU

Article 18 of Directive 2011/61/EU is replaced by the following:

'*Article 18*

General principles

1. Member States shall require that AIFMs use, at all times, adequate and appropriate human and technical resources that are necessary for the proper management of AIFs.

In particular, the competent authorities of the home Member State of the AIFM, having regard also to the nature of the AIFs managed by the AIFM, shall require that the AIFM has sound administrative and accounting procedures, control and safeguard arrangements for electronic data processing, including with regard to network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as adequate internal control mechanisms, including, in particular, rules for personal transactions by its employees or for the holding or management of investments in order to invest on its own account and ensuring, at least, that each transaction involving the AIFs may be reconstructed according to its origin, the parties to it, its nature, and the time and place at which it was effected and that the assets of the AIFs managed by the AIFM are invested in accordance with the AIF rules or instruments of incorporation and the legal provisions in force.

2. The Commission shall, by means of delegated acts in accordance with Article 56 and subject to the conditions of Articles 57 and 58, adopt measures specifying the procedures and arrangements referred to in paragraph 1 of this Article, other than the procedures and arrangements concerning network and information systems.

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).'.

Article 4

Amendments to Directive 2013/36/EU

Directive 2013/36/EU is amended as follows:

(1) in Article 65(3), point (a)(vi) is replaced by the following:

'(vi) third parties to whom the entities referred to in points (i) to (iv) have outsourced functions or activities, including ICT third-party service providers referred to in Chapter V of Regulation (EU) 2022/2554 of the European Parliament and of the Council (*);

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) in Article 74(1), the first subparagraph is replaced by the following:

'Institutions shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554, and remuneration policies and practices that are consistent with and promote sound and effective risk management.';

(3) in Article 85, paragraph 2 is replaced by the following:

'2. Competent authorities shall ensure that institutions have adequate contingency and business continuity policies and plans, including ICT business continuity policies and plans and ICT response and recovery plans for the technology they use for the communication of information, and that those plans are established, managed and tested in accordance with Article 11 of Regulation (EU) 2022/2554, in order to allow institutions to keep operating in the event of severe business disruption and limit losses incurred as a consequence of such disruption.';

(4) in Article 97(1), the following point is added:

'(d) risks revealed by digital operational resilience testing in accordance with Chapter IV of Regulation (EU) 2022/2554.'.

Article 5

Amendments to Directive 2014/59/EU

Directive 2014/59/EU is amended as follows:

(1) Article 10 is amended as follows:

(a) in paragraph 7, point (c) is replaced by the following:

'(c) a demonstration of how critical functions and core business lines could be legally and economically separated, to the extent necessary, from other functions so as to ensure continuity and digital operational resilience upon the failure of the institution;';

(b) in paragraph 7, point (q) is replaced by the following:

'(q) a description of essential operations and systems for maintaining the continuous functioning of the institution's operational processes, including network and information systems as referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council (*);

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(c) in paragraph 9, the following subparagraph is added:

'In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards in order to, inter alia, take account of the provisions of Chapter II of Regulation (EU) 2022/2554.';

(2) the Annex is amended as follows:

(a) in Section A, point (16) is replaced by the following:

'(16) arrangements and measures necessary to maintain the continuous functioning of the institution's operational processes, including network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554;';

(b) Section B is amended as follows:

(i) point (14) is replaced by the following:

'(14) an identification of the owners of the systems identified in point (13), service level agreements related thereto, and any software and systems or licenses, including a mapping to their legal entities, critical operations and core business lines, as well as an identification of critical ICT third-party service providers as defined in Article 3, point (23), of Regulation (EU) 2022/2554;';

(ii) the following point is inserted:

'(14a) the results of institutions' digital operational resilience testing under Regulation (EU) 2022/2554;';

(c) Section C is amended as follows:

(i) point (4) is replaced by the following:

'(4) the extent to which the service agreements, including contractual arrangements on the use of ICT services, that the institution maintains are robust and fully enforceable in the event of resolution of the institution;';

(ii) the following point is inserted:

'(4a) the digital operational resilience of the network and information systems supporting critical functions and core business lines of the institution, taking into account major ICT-related incident reports and the results of digital operational resilience testing under Regulation (EU) 2022/2554;'.

Article 6

Amendments to Directive 2014/65/EU

Directive 2014/65/EU is amended as follows:

(1) Article 16 is amended as follows:

(a) paragraph 4 is replaced by the following:

'4. An investment firm shall take reasonable steps to ensure continuity and regularity in the performance of investment services and activities. To that end, the investment firm shall employ appropriate and proportionate systems, including information and communication technology ("ICT") systems that are set up and managed in accordance with Article 7 of Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as appropriate and proportionate resources and procedures.

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(b) in paragraph 5, the second and third subparagraphs are replaced by the following:

'An investment firm shall have sound administrative and accounting procedures, internal control mechanisms and effective procedures for risk assessment.

Without prejudice to the ability of competent authorities to require access to communications in accordance with this Directive and Regulation (EU) No 600/2014, an investment firm shall have sound security mechanisms in place to ensure, in accordance with the requirements laid down in Regulation (EU) 2022/2554, the security and authentication of the means of transfer of information, to minimise the risk of data corruption and unauthorised access and to prevent information leakage, thereby maintaining the confidentiality of the data at all times.';

(2) Article 17 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. An investment firm that engages in algorithmic trading shall have in place effective systems and risk controls suitable to the business it operates to ensure that its trading systems are resilient and have sufficient capacity in accordance with the requirements laid down in Chapter II of Regulation (EU) 2022/2554, are subject to appropriate trading thresholds and limits and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market.

Such a firm shall also have in place effective systems and risk controls to ensure the trading systems cannot be used for any purpose that is contrary to Regulation (EU) No 596/2014 or to the rules of a trading venue to which it is connected.

The investment firm shall have in place effective business continuity arrangements to deal with any failure of its trading systems, including ICT business continuity policy and plans and ICT response and recovery plans established in accordance with Article 11 of Regulation (EU) 2022/2554, and shall ensure its systems are fully tested and properly monitored to ensure that they meet the general requirements laid down in this paragraph and any specific requirements laid down in Chapters II and IV of Regulation (EU) 2022/2554.';

(b) in paragraph 7, point (a) is replaced by the following:

'(a) the details of organisational requirements laid down in paragraphs 1 to 6, other than those related to ICT risk management, which are to be imposed on investment firms providing different investment services, investment activities, ancillary services or combinations thereof, whereby the specifications in relation to the organisational requirements laid down in paragraph 5 shall set out specific requirements for direct market access and for sponsored access in such a way as to ensure that the controls applied to sponsored access are at least equivalent to those applied to direct market access;';

(3) in Article 47, paragraph 1 is amended as follows:

(a) point (b) is replaced by the following:

'(b) to be adequately equipped to manage the risks to which it is exposed, including to manage ICT risk in accordance with Chapter II of Regulation (EU) 2022/2554, to implement appropriate arrangements and systems for identifying significant risks to its operation, and to put in place effective measures to mitigate those risks;';

(b) point (c) is deleted;

(4) Article 48 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Member States shall require a regulated market to establish and maintain its operational resilience in accordance with the requirements laid down in Chapter II of Regulation (EU) 2022/2554 to ensure its trading systems are resilient, have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, are fully tested to ensure such conditions are met and are subject to effective business continuity arrangements, including ICT business continuity policy and plans and ICT response and recovery plans established in accordance with Article 11 of Regulation (EU) 2022/2554, to ensure continuity of its services if there is any failure of its trading systems.';

(b) paragraph 6 is replaced by the following:

'6. Member States shall require a regulated market to have in place effective systems, procedures and arrangements, including requiring members or participants to carry out appropriate testing of algorithms and providing environments to facilitate such testing in accordance with the requirements laid down in Chapters II and IV of Regulation (EU) 2022/2554, to ensure that algorithmic trading systems cannot create or contribute to disorderly trading conditions on the market and to manage any disorderly trading conditions which do arise from such algorithmic trading systems, including systems to limit the ratio of unexecuted orders to transactions that may be entered into the system by a member or participant, to be able to slow down the flow of orders if there is a risk of its system capacity being reached and to limit and enforce the minimum tick size that may be executed on the market.';

(c) paragraph 12 is amended as follows:

(i) point (a) is replaced by the following:

'(a) the requirements to ensure trading systems of regulated markets are resilient and have adequate capacity, except the requirements related to digital operational resilience;';

(ii) point (g) is replaced by the following:

'(g) the requirements to ensure appropriate testing of algorithms, other than digital operational resilience testing, so as to ensure that algorithmic trading systems including high-frequency algorithmic trading systems cannot create or contribute to disorderly trading conditions on the market.'.

Article 7

Amendments to Directive (EU) 2015/2366

Directive (EU) 2015/2366 is amended as follows:

(1) in Article 3, point (j) is replaced by the following:

'(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information and communication technology (ICT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services;';

(2) Article 5(1) is amended as follows:

(a) the first subparagraph is amended as follows:

(i) point (e) is replaced by the following:

'(e) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures as well as arrangements for the use of ICT services in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), which demonstrates that those governance arrangements and internal control mechanisms are proportionate, appropriate, sound and adequate;

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(ii) point (f) is replaced by the following:

'(f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in Chapter III of Regulation (EU) 2022/2554;';

(iii) point (h) is replaced by the following:

'(h) a description of business continuity arrangements including a clear identification of the critical operations, effective ICT business continuity policy and plans and ICT response and recovery plans and a procedure to regularly test and review the adequacy and efficiency of such plans in accordance with Regulation (EU) 2022/2554;';

(b) the third subparagraph is replaced by the following:

'The security control and mitigation measures referred to in point (j) of the first subparagraph shall indicate how they ensure a high level of digital operational resilience in accordance with Chapter II of Regulation (EU) 2022/2554, in particular in relation to technical security and data protection, including for the software and ICT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations. Those measures shall also include the security measures laid down in Article 95(1) of this Directive. Those measures shall take into account EBA's guidelines on security measures as referred to in Article 95(3) of this Directive, when in place.';

(3) in Article 19(6), the second subparagraph is replaced by the following:

'Outsourcing of important operational functions, including ICT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authorities to monitor and retrace the payment institution's compliance with all of the obligations laid down in this Directive.';

(4) in Article 95(1), the following subparagraph is added:

'The first subparagraph is without prejudice to the application of Chapter II of Regulation (EU) 2022/2554 to:

(a) payment service providers referred to in points (a), (b) and (d) of Article 1(1) of this Directive;

(b) account information service providers referred to in Article 33(1) of this Directive;

(c) payment institutions exempted pursuant to Article 32(1) of this Directive; and

(d) electronic money institutions benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC.';

(5) in Article 96, the following paragraph is added:

'7. Members States shall ensure that paragraphs 1 to 5 of this Article do not apply to:

(a) payment service providers referred to in points (a), (b) and (d) of Article 1(1) of this Directive;

(b) account information service providers referred to in Article 33(1) of this Directive;

(c) payment institutions exempted pursuant to Article 32(1) of this Directive; and

(d) electronic money institutions benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC.';

(6) in Article 98, paragraph 5 is replaced by the following:

'5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments, and of the provisions of Chapter II of Regulation (EU) 2022/2554.'.

Article 8

Amendment to Directive (EU) 2016/2341

Article 21(5) of Directive (EU) 2016/2341 is replaced by the following:

'5. Member States shall ensure that IORPs take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, IORPs shall employ

appropriate and proportionate systems, resources and procedures, and shall, in particular, set up and manage network and information systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), where applicable.

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 (OJ L 333, 27.12.2022, p.1).'.

Article 9

Transposition

1. By 17 January 2025, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 17 January 2025.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

Article 10

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 11

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK