EUROPEAN
COMMISSION

Brussels, 24.9.2020
COM(2020) 596 final

2020/0268 (COD)

Proposal for a

# DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341

(Text with EEA relevance)

{SEC(2020) 309 final} - {SWD(2020) 203 final} - {SWD(2020) 204 final}

# EXPLANATORY MEMORANDUM

## 1. CONTEXT OF THE PROPOSAL

- **Reasons for and objectives of the proposal**

This proposal is part of a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. It is in line with the Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. The digital finance package includes a new Strategy on digital finance for the EU financial sector[1] with the aim to ensure that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to European consumers and businesses. In addition to this proposal, the package also includes a proposal for a regulation on markets in crypto assets[2], a proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT)[3] and a proposal for a regulation on digital operational resilience for the financial sector[4].

The reasons for, and objectives of, the two sets of legislative measures have been set out in the explanatory memoranda of the proposal for a regulation on a pilot regime for distributed ledger technology market infrastructures, proposal for a regulation on markets in crypto assets and proposal for a regulation on digital operational resilience, respectively, and apply here as well. The particular reasons for this proposal for a directive is that, in order to provide legal certainty as regards crypto assets and achieve the objectives of strengthening digital operational resilience, it is necessary to establish a temporary exemption for multilateral trading facilities and amend or clarify certain provisions in existing EU financial services directives.

- **Consistency with existing provisions in the policy area**

This proposal, similar to the proposals for regulation it accompanies, is part of a broader ongoing work at European and international level aimed at (i) strengthening the cybersecurity in financial services and address broader operational risks, and (ii) providing a clear, proportionate and enabling EU legal framework for crypto-asset service providers.

- **Consistency with other Union policies**

[1] Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, 23 September 2020, COM(2020)591.

[2] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, COM(2020) 593.

[3] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM(2020) 594.

[4] Proposal for a Regulation of the European Parliament and of the Council for operational resilience on the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020)595.

As stated by President von der Leyen in her Political Guidelines,[5] and set-out in the Communication 'Shaping Europe's digital future',[6] it is crucial for Europe to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries.

As regards crypto assets, this proposal is closely linked with wider Commission policies on blockchain technology, as crypto-assets, as the main application of blockchain technologies, are inextricably linked to the promotion of blockchain technology throughout Europe.

As regards operational resilience, the European strategy for data[7] sets out four pillars - data protection, fundamental rights, safety and cyber-security - as essential pre-requisites for a society empowered by the use of data. A legislative framework strengthening the digital operational resilience of the Union's financial entities is consistent with these policy objectives. The proposal would also support policies aimed at recovering from the coronavirus, as it would ensure that increased reliance on digital finance goes hand in hand with operational resilience. Both proposals also respond to calls from the CMU High-Level Forum to establish clear rules for the use of crypto asset (recommendation 7) and to put in place new rules on cyber resilience (recommendation 10).[8]

## 2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

This proposal for a directive is based on Articles 53(1) and 114 of the TFEU.

- **Subsidiarity (for non-exclusive competence)**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures and digital operational resilience.

- **Proportionality**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Choice of the instrument**

This proposal for a directive accompanies the proposals for a regulation on markets in crypto assets; temporary regime on DLT market infrastructures; and digital operational resilience. Those regulations lay down the key rules governing (i) crypto service providers, (ii) the conditions governing the pilot regime for DLT market infrastructures; and (iii) the key rules governing ICT risk management, incident reporting, testing and oversight. To achieve the objectives set out in those regulations, it is also necessary to establish a temporary exemption

---

5 President Ursula Von Der Leyen, *Political Guidelines for the next European Commission, 2019-2024*, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, *Shaping Europe's Digital Future*, COM(2020) 67 final.

7

8 High-Level forum on the Capital Markets Union (2020). "A new vision for Europe's capital markets: final report, https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf.

for multilateral trading facilities and to amend several Directives of the European Parliament and of the Council adopted on the basis of Articles 53(1) and 114 of the TFEU. This proposal for a Directive is therefore required to amend these Directives.

## 3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and digital operational resilience.

- **Stakeholder consultations**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Collection and use of expertise**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Impact assessment**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Regulatory fitness and simplification**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Fundamental rights**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

## 4. BUDGETARY IMPLICATIONS

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures and digital operational resilience.

## 5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

See the explanatory memorandums of the proposals for regulation on markets in crypto assets, temporary regime on DLT market infrastructures; and, digital operational resilience.

- **Detailed explanation of the specific provisions of the proposal**

All Articles relate to and complement the proposal for a regulation on digital operational resilience. They amend the various operational risk or risk management requirements foreseen in Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 of the European Parliament and of the

Council, by introducing precise cross-references in those provisions and thus attain legal clarity. More specifically:

– Articles 2 to 4, 6 and 8 amend Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)[9], Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II),[10] Directive 2011/61/EU on Alternative Investment Fund Managers (AIFMD),[11] Directive 2014/56/EU on statutory audits of annual accounts and consolidated accounts,[12] and Directive EU/2016/2341 on the activities and supervision of institutions for occupational retirement provision (IORPs),[13] and with the purpose of introducing in each of those directives specific cross-references to Regulation (EU) 2021/xx [DORA] for these financial entities' management of ICT systems and tools that should be done in accordance with the provisions of that Regulation.

– Article 5 amends the requirements in Directive 2013/36/EU (the Capital Requirements Directive, CRD)[14] on contingency and business continuity plans to include ICT business continuity and disaster recovery plans established in accordance with the provisions laid down in Regulation (EU) 2021/xx [DORA];

– Article 6 amends Directive 2014/65/EU on markets in financial instruments (MIFID2) by adding cross-references to Regulation (EU) 2021/xx [DORA] and by amending provisions relating to continuity and regularity in the performance of investment services and activities, resilience and sufficient capacity of trading systems, effective business continuity arrangements and risk management;

– Article 7 amends Directive (EU) 2015/2366 on payment services in the internal market (PSD2)[15] and more precisely the authorisation rules by introducing a cross-reference to Regulation (EU) 2021/xx [DORA]. In addition, the incident notification rules in that Directive should exclude ICT-related incident notification that Regulation (EU) 2021/xx [DORA] fully harmonises;

---

9 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 (OJ L 302, 17.11.2009, p. 32).

10 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 (OJ L 335, 17.12.2009, p. 1).

11 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).

12 Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (OJ L 158, 27.5.2014, p. 196).

13 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 (OJ L 354, 23.12.2016, p. 37).

14 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

15 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).

The first paragraph of Article 6 further contributes to clarifying the legal treatment of crypto assets qualifying as financial instruments. It does so by amending the definition of a 'financial instrument' in Directive 2014/65/EU on markets in financial instruments to clarify beyond any legal doubt that such instruments can be issued on a distributed ledger technology.

The fourth paragraph of Article 6 complements the proposal for a regulation on a pilot regime for distributed ledger technology market infrastructures by temporarily exempting distributed ledger technology market infrastructures from certain provisions in Directive 2014/65/EU in order enable them to develop solutions for the trading and settlement of transactions of crypto-assets that would qualify as financial instruments.

2020/0268 (COD)

Proposal for a

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341**

(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,[16]

Having regard to the opinion of the European Economic and Social Committee,[17]

Acting in accordance with the ordinary legislative procedure,

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.

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

(3) At Union level the requirements related to ICT risk for the financial sector are currently spread over Directives 2006/43/EC,[18] 2009/66/EC,[19] 2009/138/EC,[20]

16 OJ C …, …, p. 1…

17 OJ C , , p. .

18 Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).

19 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).

20 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) .

2011/61/EC,[21] EU/2013/36,[22] 2014/65/EU,[23] (EU) 2015/2366,[24] (EU) 2016/2341[25] of the European Parliament and of the Council and are diverse and occasionally incomplete. In some cases, ICT risk has only been implicitly addressed as part of the operational risk, whereas in others it has not been addressed at all. This should be remedied by aligning Regulation (EU) xx/20xx of the European Parliament and of the Council[26] [DORA] and those acts. This Directive puts forward a set of amendments that appear necessary to bring legal clarity and consistency in relation to the application by financial entities that are authorised and supervised in accordance with those Directives of various digital operational resilience requirements that are necessary in the pursuit of their activities, thus guaranteeing the smooth functioning of the internal market.

(4) In the area of banking services, Directive 2013/36/EU on access to the activity of credit institutions and the prudential regulation of credit institutions and investment firms 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 management. However, to ensure that ICT risk is explicitly addressed, the requirements for contingency and business continuity plans should be amended to include business continuity and disaster recovery plans also for ICT risk, in in accordance with the requirements laid down in Regulation (EU) 2021/xx [DORA].

(5) Directive 2014/65/EU on markets in financial instruments sets out more stringent ICT rules for investment firms and trading venues only when performing algorithmic trading. Less detailed requirements apply to data reporting services and to trade repositories. Also, it only contains limited references to control and safeguard arrangements for the information processing systems and on use of appropriate systems, resources and procedures to ensure continuity and regularity of business services. That Directive should be aligned with Regulation (EU) 2021/xx [DORA] as regards continuity and regularity in the performance of investment services and activities, operational resilience, capacity of trading systems, and effectiveness of business continuity arrangements and risk management.

---

21 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).

22 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

23 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).

24 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).

25 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).

26 OJ L […], […], p. […].

(6) Currently, the definition of 'financial instrument' in Directive 2014/65/EU does not explicitly include financial instruments issued using a class of technologies which support the distributed recording of encrypted data (distributed ledger technology, "DLT"). In order to ensure that such financial instruments can be traded on the market under the current legal framework, the definition in Directive 2014/65/EU should be amended to include them.

(7) In particular, in order to allow for the development of crypto-assets that would qualify as financial instruments and DLT, while preserving a high level of financial stability, market integrity, transparency and investor protection, it would be beneficial to create a temporary regime for DLT market infrastructures. This temporary legal framework should allow competent authorities to temporarily permit DLT market infrastructures to operate under an alternative set of requirements with regard to access to them compared to those otherwise applicable under the Union financial services legislation that could prevent them from developing solutions for the trading and settlement of transactions of crypto-assets that would qualify as financial instruments. This legal framework should be temporary in order to enable the European Supervisory Authorities (ESAs) and the national competent authorities to gain experience on the opportunities and specific risks created by crypto-assets traded on those infrastructures. This Directive is consequently accompanying Regulation [on a pilot regime for market infrastructures based on distributed ledger technology] by supporting this new Union regulatory framework on DLT market infrastructures with a targeted exemption from specific provisions of Union financial services legislation applying to activities and services in relation to financial instruments as defined in point (15) of Article 4(1) of Directive 2014/65/EU that would otherwise not offer the full flexibility required when deploying solutions in the trading and post trading stages of transactions involving crypto-assets.

(8) A DLT multilateral trading facility should be a multilateral system, operated by an investment firm or a market operator authorised under Directive 2014/65/EU, that has received a specific permission under Regulation (EU) xx/20xx of the European Parliament and of the Council[27] [Proposal for a regulation on a pilot regime on DLT market infrastructure]. DLT multilateral trading facilities should be subject to all the requirements applicable to a multilateral trading facility under that Directive, except if it were to be granted an exemption by its national competent authority in accordance with this Directive. One potential regulatory barrier to the development of a multilateral trading facility for transferable securities issued on a DLT could be the obligation of intermediation set out in Directive 2014/65/EU. A traditional multilateral trading facility can only admit as members and participants investment firms, credit institutions and other persons who have a sufficient level of trading ability and competence and who dispose of appropriate organisational arrangements and resources. A DLT multilateral trading facility should be allowed to request a derogation from such an obligation so that is can provide retail investors with easy access to the trading venue, provided that adequate safeguards are in place in terms of investor protection.

(9) Directive (EU) 2015/2366 on payment services sets out specific rules on ICT security controls and mitigation elements for the purposes of authorisation to perform payment services. Those authorisation rules should be amended in order to align

[27] [full title] (OJ L […], […], p. […]).

them with to Regulation (EU) 2021/xx [DORA]. Furthermore, the incident notification rules in that Directive should not apply to ICT-related incident notifications that Regulation (EU) 2021/xx [DORA] fully harmonises.

(10) Directives 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance and EU/2016/2341 on the activities and supervision of institutions for occupational retirement provision partially capture ICT risk within their general provisions on governance and risk management, leaving certain requirements to be specified through delegated regulations with or without specific references to ICT risk. Even less specific provisions apply to statutory auditors and audit firms as Directive 2014/56/EU of the European Parliament and of the Council[28] only contains general provisions on internal organisation. Similarly, only very general rules apply to managers of alternative investment funds and management companies subject to Directives 2011/61/EU and 2009/65/EC. These Directives should therefore be aligned with the requirements laid down in Regulation (EU) 2021/xx [DORA] with regard to the management of ICT systems and tools.

(11) In many cases, further ICT requirements have been already laid down in delegated and implementing acts, which have been adopted on the basis of draft technical regulatory and implementing technical standards developed by the competent ESA. In order to provide legal clarity about the fact that the legal base of ICT risk provisions henceforth exclusively derives from Regulation (EU) 2021/xx [DORA], the empowerments in these Directives should be amended explaining that ICT risk provisions fall outside the scope of those empowerments.

(12) To ensure a consistent and simultaneous application of Regulation xx/20xx [DORA] and of this Directive, which together constitute 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 that Regulation.

(13) Directives 2006/43/EC, 2009/66/EC, 2009/138/EC, 2011/61/EC, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 have been adopted on the bases of Article 53(1) and 114 of the Treaty on the Functioning of the European Union. The amendments in this Directive should be included in a single act due to the interconnectedness of the subject matter and objectives of the amendments, and this single act should be adopted on the basis of both Article 53(1) and 114 of the Treaty on the Functioning of the European Union.

(14) Since the objectives of this Directive cannot be sufficiently achieved by the Member States as they entail the harmonisation through updates and amendments of requirements already contained in Directives but can rather, by reason of both 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 Regulation does not go beyond what is necessary in order to achieve those objectives.

[28] Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (OJ L 158, 27.5.2014, p. 196).

(15) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents[29], 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 2006/43/EC***

In Article 24a(1) of Directive 2006/43/EC, point (b) is replaced by the following:

'(b) a statutory auditor or an audit firm shall have sound administrative and accounting procedures, internal quality control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements in order to manage its ICT systems and tools in accordance with Article 6 of Regulation (EU) 2021/xx [DORA] of the European Parliament and of the Council*.

_____

* [*full title*] (OJ L […], […], p. […]).'.

*Article 2*

***Amendments to Directive 2009/65/EC***

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

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

'(a) has sound administrative and accounting procedures and control and safeguard arrangements for electronic data processing, including information and communication technology systems that are set up and managed in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA], as well as adequate internal control mechanisms including rules for personal transactions by its employees or for the holding and 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;

_____

[29] OJ C 369, 17.12.2011, p. 14.

* [*full title*] (OJ L […], […], p. […]).';

(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 those related to information and communication technology risk management;

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

*Article 3*

***Amendment 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 undertaking shall employ appropriate and proportionate systems, resources and procedures and shall set up information communication technology systems and manage them in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].';

---

* [*full title*] (OJ L […], […], p. […]).

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

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

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

*Article 4*

***Amendments to Directive 2011/61/EC***

Article 18 of Directive 2011/61/EC 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 managing the information communication technology systems required by Article 6 of [Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA]], 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, other than for information communication technology systems.

---

* [*full title*] (OJ L […], […], p. […]).'.

*Article 5*

***Amendment to Directive 2013/36/EU***

In Article 85 of Directive 2013/36/EU, paragraph 2 is replaced by the following:

'2. Competent authorities shall ensure that institutions have adequate contingency and business continuity plans, including business continuity and disaster recovery plans for the technology they use for the communication of information ("information communication technology") established in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA] of the European Parliament and of the Council * , for them to keep operating in the event of severe business disruption and limit losses incurred as a consequence of such a disruption..

---

* [*full title*] (OJ L […], […], p. […]).'

*Article 6*

***Amendments to Directive 2014/65/EU***

Directive 2014/65/EU is amended as follows:

(1) in Article 4(1), point 15 is replaced by the following:

‘financial instrument’ means those instruments specified in Section C of Annex I, including such instruments issued by means of distributed ledger technology;’;

(2) 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 communication technology (“ICT”) systems set up and managed in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA], as well as appropriate and proportionate resources and procedures.’;

(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 guarantee, in accordance with the requirements laid down in Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA], the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining the confidentiality of the data at all times.’;

(3) 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) 2021/xx [DORA], 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 business continuity and disaster recovery plans for information communication technology established in accordance Article 6 of Regulation (EU) 2021/xx [DORA], 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) 2021/xx [DORA].’;

(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;';

(4) in Article 19, the following paragraph is added:

"3. However, where the investment firm or market operator operates a distributed ledger technology multilateral trading facility ("DLT multilateral trading facility") as defined in Article 2(3) of Regulation xx/20xx [proposal for a regulation on a pilot regime for DLT market infrastructure], the competent authority may permit that, under its rules governing access as referred to in Article 18(3) and for a maximum of four years, the investment firm or market operator admits natural persons to the DLT multilateral trading facility as members or participants, provided that those persons fulfil the following requirements:

(a) they must be of sufficient good repute and fit and proper; and

(b) they must have sufficient level of trading ability, competence and experience, including knowledge of trading and the functioning of distributed ledger technology ("DLT").

Where a competent authority grants the exemption referred to in the first subparagraph, it may impose additional investor protection measures for the protection of natural persons admitted as members or participants to the DLT multilateral trading facility. Such measures shall be proportionate to the risk profile of the participants or members."

(5) 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 risks to the ICT systems and tools in accordance with Article 6 of Regulation (EU) 2021/xx [DORA]*, to implement appropriate arrangements and systems for identifying all significant risks to its operation, and to put in place effective measures to mitigate those risks.';

(b) point (c) is deleted;

(6) Article 48 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Member States shall require a regulated market to build its operational resilience in accordance with the requirements laid down in Chapter II of Regulation (EU) 2021/xx [DORA] 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 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) 2021/xx [DORA], 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:

(7) In Article 5(1), in the third subparagraph, the first sentence 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 technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations, in accordance with Chapter II of Regulation (EU) 2021/xx of the European Parliament and of the Council * [DORA].Those measures shall also include the security measures laid down in Article 95(1). Those measures shall take into account EBA's guidelines on security measures as referred to in Article 95(3) when in place.';

---

* [full title] (OJ L […], […], p. […]).

(8) Article 95 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide and, as part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents, while addressing risks to

information communication technology in accordance with Chapter II of Regulation (EU) 2021/xx [DORA].';

(b) paragraph 4 is deleted;

(c) paragraph 5 is replaced by the following:

'5. EBA shall promote cooperation, including the sharing of information, in the area of operational risks associated with payment services among the competent authorities, and between the competent authorities and the ECB.';

(9) Article 96 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. In case of a major operational or security incident that is not an ICT-related incident as defined in Article 3(6) of Regulation (EU) xx/20xx [DORA], the payment service provider shall, without undue delay, notify the competent authority in its home Member State.';

(b) paragraph 5 is deleted;

(10) 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) 2021/xx [DORA].'.

*Article 8*

***Amendment to Directive (EU) 2016/2341***

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

'To that end, IORPs shall employ appropriate and proportionate systems, resources and procedures and shall set up ICT systems and tools and manage them in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].

---

* [*full title*] (OJ L […], […], p. […]).'.

*Article 9*

***Transposition***

1. Member States shall adopt and publish, by [one year after adoption] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of those provisions.

They shall apply those provisions from [date of entry into force of DORA/its date of application, if different].

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions 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 Brussels,

| | |
|---|---|
| *For the European Parliament* | *For the Council* |
| *The President* | *The President* |