***I

REPORT


Committee on Economic and Monetary Affairs

Rapporteur: Mikuláš Peksa
### Symbols for procedures

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Consultation procedure</td>
</tr>
<tr>
<td>***</td>
<td>Consent procedure</td>
</tr>
<tr>
<td>***I</td>
<td>Ordinary legislative procedure (first reading)</td>
</tr>
<tr>
<td>***II</td>
<td>Ordinary legislative procedure (second reading)</td>
</tr>
<tr>
<td>***III</td>
<td>Ordinary legislative procedure (third reading)</td>
</tr>
</tbody>
</table>

(The type of procedure depends on the legal basis proposed by the draft act.)

### Amendments to a draft act

#### Amendments by Parliament set out in two columns

Deletions are indicated in *bold italics* in the left-hand column. Replacements are indicated in *bold italics* in both columns. New text is indicated in *bold italics* in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

#### Amendments by Parliament in the form of a consolidated text

New text is highlighted in *bold italics*. Deletions are indicated using either the *symbol or strikethrough. Replacements are indicated by highlighting the new text in *bold italics* and by deleting or striking out the text that has been replaced.

By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION</td>
<td>4</td>
</tr>
<tr>
<td>OPINION OF THE COMMITTEE ON LEGAL AFFAIRS</td>
<td>22</td>
</tr>
<tr>
<td>PROCEDURE – COMMITTEE RESPONSIBLE</td>
<td>32</td>
</tr>
<tr>
<td>FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE</td>
<td>33</td>
</tr>
</tbody>
</table>
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION


(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2020)0596),

– having regard to Article 294(2) and Articles 53(1) and 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0303/2020),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Central Bank of 4 June 2021,¹

– having regard to the opinion of the European Economic and Social Committee of 24 February 2021,²

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the opinion of the Committee on Legal Affairs,

– having regard to the report of the Committee on Economic and Monetary Affairs (A9-0340/2021),

1. Adopts its position at first reading hereinafter set out;

2. Suggests that the act be cited as ‘the DORA directive’;

3. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

4. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

----------------------------------------------------------------------
2020/0268(COD)

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL


(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 Articles 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,

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 ensuring that further support is provided to the potential of digital finance in terms of innovation and competition.

(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.

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

¹ OJ C ..., ..., p. 1...
² OJ C , , p..
At Union level the requirements related to ICT risk for the financial sector are currently spread over Directives 2006/43/EC, 2009/66/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366, and (EU) 2016/2341 of the European Parliament and of the Council and are diverse and occasionally incomplete. The existing provisions of Union law are not fully harmonised and it is necessary to avoid over-regulation and to guarantee the adequacy of those provisions with regard to the reality in the field, which is constantly evolving. 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 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, while encouraging proportionality in particular with regard to SMEs, other small financial entities, and other microenterprises, with the aim of reducing compliance costs.

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, and in order to provide legal clarity, the requirements for contingency and business continuity plans should be amended in a proportionate way to include business continuity and disaster recovery plans also for ICT risk, in accordance with the requirements laid down in Regulation (EU) 2021/xx [DORA]. Furthermore, ICT risk is only implicitly included in the supervisory review of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).


11 OJ L […], […], p. […].
and evaluation process (SREP) performed by competent authorities as part of operational risk management and the criteria for its assessment are currently defined in the guidelines of the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council\(^\text{12}\). In order to provide legal clarity and ensure that bank supervisors effectively identify and monitor ICT risks in line with the new framework on digital operational resilience, the scope of the SREP should be amended to explicitly include the requirements laid down in Regulation (EU) 2021/xx [DORA] and cover in particular the risks revealed by major ICT-related incident reports and by the results of the digital operational resilience tests performed by institutions in accordance with that Regulation.

(4a) Digital operational resilience is an essential condition in order to preserve the critical functions and core business lines of an institution 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 an institution to continue operating and can jeopardise resolution objectives. Relevant ICT service contracts are also essential in order to ensure operational continuity and 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 institutions’ resolvability.

(4b) Establishing and maintaining adequate network and information system infrastructures is also a fundamental precondition for effective risk data aggregation and risk reporting practices, which are in turn an essential requisite for the sound and sustainable risk management and decision-making processes of credit institutions. At international level, the Basel Committee on Banking Supervision (BCBS) published in 2013 a set of principles for effective risk data aggregation and risk reporting (BCBS 239) based on two overarching principles of governance and IT infrastructure. Global systemically important banks were required to implement those principles by the beginning of 2016. However, the Report of the European Central Bank (ECB) of May 2018 on the Thematic Review on effective risk data aggregation and risk reporting and the BCBS Progress Report of April 2020 found that the implementation progress made by global systemically important banks was unsatisfactory and a source of concern. In order to facilitate compliance and alignment with international standards, the Commission, in close cooperation with the ECB and after consulting EBA and the European Systemic Risk Board (ESRB), should produce a report to assess how the BCBS 239 principles interact with the provisions of Regulation (EU) 2021/xx [DORA] and if appropriate how those principles should be incorporated into Union law.

(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.

(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 those crypto-assets that qualify as financial instruments are covered by the existing Union financial services law and that they are subject to the same requirements applicable to traditional financial instruments, regardless of the technology used for their issuance or transfer, the definition in Directive 2014/65/EU should be amended to include them.

(7) 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 them with to Regulation (EU) 2021/xx [DORA]. Furthermore, in order to reduce the administrative burden and avoid complexity and duplicative reporting requirements, the incident notification rules in that Directive should cease to apply for payment service providers that fall within the scope of Chapter III of Regulation (EU) 2021/xx [DORA], thus creating a single and fully harmonised incident reporting mechanism for payment service providers with regard to all operational and security incidents, both payment-related and not payment-related.

(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 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.

(10a) Ensuring operational resilience is crucial to strengthening the ability of financial institutions to combat money laundering and terrorist financing, especially in light of the increasing and emerging risks opened up in the post-COVID environment, where it is easier for criminals to exploit weaknesses and gaps in institutions’ systems and controls. To ensure that the digital operational resilience dimension is

---

adequately addressed in the context of combating money laundering and terrorist financing, Directive (EU) 2015/849 should be amended to explicitly include, in respect of obliged entities that fall within the scope of Regulation (EU) 2021/xx [DORA], digital operational resilience requirements as part of the policies, controls and procedures put in place by those obliged entities to mitigate and manage effectively the risks related to money laundering and terrorist financing.

(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.

(15) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, 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, the following point is inserted:

‘(ba) a statutory auditor or an audit firm which is not a micro, small or medium-sized enterprise, except if it audits entities listed in Article 2 of Regulation (EU) 2021/xx [DORA], 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 network and information and communication technology systems that are set up and managed in accordance with 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;

* [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:

Pe689.790v02-00 10/33 RR\1245018EN.docx EN
(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, in particular network and information systems and manage them in accordance with Chapter II 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, 47 and 48, other than functions related to information communication technology risk management.’.
Article 4
Amendments to Directive 2011/61/EU

Directive 2011/61/EU is amended as follows:

(1) in Article 6(4), the following point is added to point (b):

'iv) any other ancillary service where the ancillary service represents a continuation of the services already undertaken by the AIFM or a use of internal competences, and does not create conflicts of interest that could not be managed by additional rules.'

(1) 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 managing the network and information systems in accordance with [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

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) 2021/xx of the European Parliament and of the Council [DORA]*;’;

(-1a) 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) 2021/xx of the European Parliament and of the Council [DORA], and remuneration policies and practices that are consistent with and promote sound and effective risk management.’;

(-1b) in Article 85(1), paragraph 1 is replaced by the following:
‘1. Competent authorities shall ensure that institutions implement policies and processes to identify, monitor and manage the exposures to operational risk, including risks resulting from outsourcing and sub-outsourcing of functions and ICT third-party risk as defined in Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA], to model risk and to cover low-frequency high-severity events. Institutions shall identify the main sources of operational risk for the purposes of those policies and procedures.’;

(1) 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 ICT business continuity policy and disaster recovery plans established, managed and tested in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA], 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. […]).’

(1a) Article 97 is amended as follows:

(1) in paragraph 1, the following point is inserted:
‘(b) risks revealed by digital operational resilience testing in accordance with Chapter IV of Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA];’

(2) paragraph 2 is replaced by the following:
‘2. The scope of the review and evaluation referred to in paragraph 1 shall cover all the requirements of this Directive and of Regulation (EU) No 575/2013 as well as the requirements laid down in Regulation (EU) 2021/xx of the European Parliament and of the Council*[DORA].’.
Article 5a

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 established in accordance with Regulation (EU) 2021/xx [DORA];’;

(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, inter alia, to take account of the provisions of Chapter II of Regulation (EU) 2021/xx [DORA].’;

(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) 2021/xx [DORA];’;

(b) in Section B, 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 the identification of critical third-party ICT service providers;’;

(c) in Section B, the following point is inserted:

‘(14a) institutions’ major ICT-related incident reports and the results of digital operational resilience tests under Regulation XX [DORA];’;

(d) in Section C, point (4) is replaced by the following:
‘(4) the extent to which the service agreements, including ICT service contracts, that the institution maintains are robust and fully enforceable in the event of resolution of the institution;’

(e) in Section C, the following point is inserted:

‘(4a) the extent to which the institution is capable of restoring and maintaining the network and information systems that support critical functions and core business lines of the institution, taking into account major ICT-related incident reports and the results of digital operational resilience tests under Regulation XX [DORA].’

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 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 risks in accordance with Chapter II of Regulation (EU) 2021/xx [DORA]*, 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;

(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, which shall include ICT business continuity policy and disaster recovery plans established in accordance
with Regulation (EU) 2021/xx (DORA), 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 6a (new)

Amendments to Directive (EU) 2015/849

Directive (EU) 2015/849 is amended as follows:

(1) in Article 7(4), the following point is added:

'(h) take appropriate steps to support procedures in accordance with Chapter II of Regulation (EU) 2021/xx [DORA] in relation to mitigating ICT-related risks, where applicable.’;

(2) in Article 8(4), the following point is added:

(c) where applicable, the requirements concerning the security of network and information systems supporting the policies, controls and procedures referred to in point (a) of this paragraph, that are set up and managed in accordance with the requirements laid down in Chapter II of Regulation (EU) 2021/xx [DORA].’.
Directive (EU) 2015/2366 is amended as follows:

(-1a) in Article 5(1), the first subparagraph is amended as follows:

(a) 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) 2021/xx of the European Parliament and of the Council* [DORA], which demonstrates that those governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;’;

(b) 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) 2021/xx of the European Parliament and of the Council * [DORA];’;

(c) 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 disaster recovery plans and a procedure to regularly test and review the adequacy and efficiency of such plans in accordance with Regulation (EU) 2021/xx [DORA];’;

(I) 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. […]).’;

(1a) in Article 20, paragraph 1 is replaced by the following:

‘1. Member States shall ensure that, where payment institutions rely on third parties for the performance of operational functions or activities, those payment institutions take reasonable steps to ensure that the requirements of this Directive and of Chapter V of Regulation (EU) 2021/xx of the European Parliament and of the Council*
(1b) **in Article 22, paragraph 1 is replaced by the following:**

‘1. Member States shall designate as the competent authorities responsible for the authorisation and prudential supervision of payment institutions which are to carry out the duties provided for under this Title and in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA] either public authorities, or bodies recognised by national law or by public authorities expressly empowered for that purpose by national law, including national central banks.’;

(2) **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, where applicable, 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, ENISA and the ECB.’;

(3) **Article 96 is amended as follows:**

(a) **(aa) the following paragraph is inserted:**

‘(2a) Paragraphs 1 and 2 of this Article shall not apply to the payment service providers referred to in points (a), (b) and (d) of Article 1(1), which are subject to the reporting obligations of Chapter III of Regulation (EU) 2021/xx [DORA].’;

(b) paragraph 5 is deleted;

(4) **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, *in particular network and information* systems, and manage them in accordance with Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA], *where applicable.*

* [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  
The President

For the Council  
The President
6.7.2021

OPINION OF THE COMMITTEE ON LEGAL AFFAIRS

for the Committee on Economic and Monetary Affairs


Rapporteur for opinion (*): Mislav Kolakušić

(*) Associated committee – Rule 57 of the Rules of Procedure

SHORT JUSTIFICATION

This Commission legislative proposal is part of a package of measures that, at the same time, supports the potential of digital finance in the context of innovation and competition, while mitigating risks. It is in line with the Commission's priorities of preparing Europe for the digital age and building an economy that will be ready to meet the challenges of the future and forms part of the wider activities carried out at European and international level with a view to strengthening cybersecurity in the area of financial services and eliminating operational risks while introducing a clear, proportionate and enabling legal framework for crypto-property service providers.

European Union must respond comprehensively to any digital risks to which financial entities are exposed, risks arising from the rapidly growing use of information and communication technology (ICT) in the provision and use of financial services. The financial sector today relies heavily on digital technologies, a dependence on digital technology products that will only become more prominent, and it is of paramount importance to ensure that their digital operations are guaranteed to be operationally resilient to ICT risks. Operational resilience is also becoming a key factor due to the growth of advanced technologies market, primarily based on the possibility for digital representations of values or rights to be electronically transmitted and stored using decentralised ledger technology or similar technology ('crypto-assets'), and services related to such assets.

The rapporteur's views

The Commission proposal would lead to a limitation in the obligations of statutory auditors and audit firms, as in the future these obligations would relate exclusively to ICT and not to a statutory auditor or audit firms procedures and organisation in general. As a result, a new point has been proposed that undoubtedly indicates that the existing obligations of audit firms remain in force, and that new ones relating to ICT are added.
Compliance with Article 6. Regulation (EU) 2021/xx [DORA] of the European Parliament and the Council is not possible due to the fact that such a Regulation is not in force and does not exist legally. Such a solution incorporating into the proposal for a directive only the text of the article referred to by the Commission is only legally possible, while at the same time achieving the purpose and objective of the European Commission's proposal, as the effects are identical to those of the Commission.

Given that the DORA Regulation is still at the proposal stage and has not been adopted by the European Parliament and Council, there is a legal problem of harmonisation of the Directives in question with the provisions of the Regulation which is not legally and effectively in force. Given that the final content and rules established by that Regulation will not be known until the entry into force of DORA, it is legally untenable to harmonise those directives with a regulation that does not exist legally and effectively at the moment.

**AMENDMENTS**

The Committee on Legal Affairs calls on the Committee on Economic and Monetary Affairs, as the committee responsible, to take into account the following amendments:

**Amendment 1**

**Proposal for a directive**

**Recital 1**

*Text proposed by the Commission*

(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.

*Amendment*

(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, ensuring further support is provided to the potential of digital finance in terms of innovation and competition.

**Amendment 2**

**Proposal for a directive**

**Recital 3**

RR\1245018EN.docx
(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 2011/61/EC,21 EU/2013/36,22 2014/65/EU,23 (EU) 2015/2366,24 (EU) 2016/234125 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 Council26 [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.

---


26 OJ L […]], […]], p. […]].
Amendment 3
Proposal for a directive
Recital 6

Text proposed by the Commission

(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.

Amendment

(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”), thus not reflecting the reality of the market. In order to ensure that such financial instruments can be traded on the market under the current legal framework, in order to avoid any potential risk due to non-regulation, the definition in Directive 2014/65/EU should be amended to include them.

Amendment 4
Proposal for a directive
Recital 7

Text proposed by the Commission

(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

Amendment

(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 and consumer 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.
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.

Amendment 5
Proposal for a directive
Recital 13 a (new)

*Text proposed by the Commission*

(13a) The regulatory process should take into account the proper balance between, on the one hand, efficient management of risk limitation and, on the other hand, ensuring fair competition in terms of encouraging the development of innovation in the market and protecting all actors involved.
Amendment 6
Proposal for a directive
Article 1 – paragraph 1
Directive 2006/43/EC
Article 24a – paragraph 1 – point b

Text proposed by the Commission
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. […]).’.

Amendment 7
Proposal for a directive
Article 1 – paragraph 1
Directive 2006/43/EC
Article 24a – paragraph 1 – point b a (new)

Text proposed by the Commission
In Article 24a(1) of Directive 2006/43/EC, the following point is inserted:

(ba) a statutory auditor or an audit firm which is not a micro, small or medium-sized enterprise, except if it audits entities listed in Article 2 of Regulation (EU) 2021/xx [DORA], 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
Amendment 8

Proposal for a directive
Article 2 – paragraph 1 – point 1
Directive 2009/65/EC
Article 12 – paragraph 1 – subparagraph 2 – point a

**Text proposed by the Commission**

(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;

**Amendment**

(a) has sound administrative, operational 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;

* [full title] (OJ L […], […], p. […]).’
**PROCEDURE – COMMITTEE ASKED FOR OPINION**

| Committee responsible | Date announced in plenary | ECON 17.12.2020 |
| Opinion by | Date announced in plenary | JURI 17.12.2020 |
| Associated committees - date announced in plenary | 11.2.2021 |
| Rapporteur for the opinion | Date appointed | Mislav Kolakušić 10.5.2021 |
| Discussed in committee | 27.5.2021 |
| Date adopted | 1.7.2021 |
| Result of final vote | +: 23|
| | -: 0|
| | 0: 2|
| Members present for the final vote | Pascal Arimont, Manon Aubry, Gunnar Beck, Geoffroy Didier, Pascal Durand, Angel Dzhambazki, Ibán García Del Blanco, Jean-Paul Garraud, Esteban González Pons, Mislav Kolakušić, Sergey Lagodinsky, Gilles Lebreton, Karen Melchior, Jiří Pospíšil, Franco Roberti, Marcos Ros Sempere, Stéphane Séjourné, Raffaele Stancanelli, Marie Toussaint, Axel Voss, Marion Walsmann, Tiemo Wölken, Lara Wolters, Javier Zarzalejos |
| Substitutes present for the final vote | Magdalena Adamowicz, Caterina Chinnici, Heidi Hautala, Emmanuel Maurel, Emil Radev, Yana Toom |
### FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>+</td>
</tr>
<tr>
<td>PPE</td>
<td>Pascal Arimont, Geoffroy Didier, Esteban González Pons, Jiří Pospíšil, Axel Voss, Marion Walsmann, Javier Zarzalejos</td>
</tr>
<tr>
<td>S&amp;D</td>
<td>Ibán García Del Blanco, Franco Roberti, Marcos Ros Sempere, Tiemo Wölken, Lara Wolters</td>
</tr>
<tr>
<td>Renew</td>
<td>Pascal Durand, Karen Melchior, Stéphane Séjourné, Yana Toom</td>
</tr>
<tr>
<td>ID</td>
<td>Jean-Paul Garraud, Gilles Lebreton</td>
</tr>
<tr>
<td>Verts/ALE</td>
<td>Heidi Hautala, Marie Toussaint</td>
</tr>
<tr>
<td>ECR</td>
<td>Angel Dzhambazki, Raffaele Stancanelli</td>
</tr>
<tr>
<td>The Left</td>
<td>Emmanuel Maurel</td>
</tr>
<tr>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>ID</td>
<td>Gunnar Beck</td>
</tr>
<tr>
<td>NI</td>
<td>Mislav Kolakušić</td>
</tr>
</tbody>
</table>

Key to symbols:
+ : in favour
- : against
0 : abstention
### PROCEDURE – COMMITTEE RESPONSIBLE

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date submitted to Parliament</td>
<td>24.9.2020</td>
</tr>
<tr>
<td>Committee responsible</td>
<td>ECON</td>
</tr>
<tr>
<td>Date announced in plenary</td>
<td>17.12.2020</td>
</tr>
<tr>
<td>Committees asked for opinions</td>
<td>ITRE IMCO JURI</td>
</tr>
<tr>
<td>Not delivering opinions</td>
<td>ITRE IMCO</td>
</tr>
<tr>
<td>Date of decision</td>
<td>15.10.2020 27.10.2020</td>
</tr>
<tr>
<td>Associated committees</td>
<td>JURI</td>
</tr>
<tr>
<td>Date announced in plenary</td>
<td>11.2.2021</td>
</tr>
<tr>
<td>Rapporteurs</td>
<td>Mikuláš Peksa</td>
</tr>
<tr>
<td>Date appointed</td>
<td>15.10.2020</td>
</tr>
<tr>
<td>Discussed in committee</td>
<td>14.4.2021 14.6.2021</td>
</tr>
<tr>
<td>Date adopted</td>
<td>1.12.2021</td>
</tr>
<tr>
<td>Result of final vote</td>
<td>++: 44 −: 5 0: 5</td>
</tr>
<tr>
<td>Substitutes present for the final vote</td>
<td>Lefteris Christoforou</td>
</tr>
<tr>
<td>Date tabled</td>
<td>7.12.2021</td>
</tr>
</tbody>
</table>
# FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>+</strong></td>
<td></td>
</tr>
<tr>
<td>ECR</td>
<td>Raffaele Fitto, Johan Van Overtveldt, Roberts Zile</td>
</tr>
<tr>
<td>NI</td>
<td>Enikő Győri</td>
</tr>
<tr>
<td>PPE</td>
<td>Isabel Benjumea Benjumea, Stefan Berger, Leftferis Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lidia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere</td>
</tr>
<tr>
<td>Renew</td>
<td>Gilles Boyer, Engin Eroğlu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin</td>
</tr>
<tr>
<td>Verts/ALE</td>
<td>Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun</td>
</tr>
</tbody>
</table>

| **-** |     |
| ID | Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen |
| NI | Leftferis Nikolaou-Alavanos |

| **0** |     |
| ID | Valentino Grant, Antonio Maria Rinaldi, Marco Zanni |
| The Left | José Gusmão, Martin Schirdewan |

**Key to symbols:**
+ : in favour  
- : against  
0 : abstention