DRAFT REPORT


Committee on Economic and Monetary Affairs

Rapporteur: Mikuláš Peksa

Rapporteurs for the opinion (*): xxx, Committee on Legal Affairs

(*) Associated committees – Rule 57 of the Rules of Procedure
Symbols for procedures

* Consultation procedure
*** Consent procedure
***I Ordinary legislative procedure (first reading)
***II Ordinary legislative procedure (second reading)
***III Ordinary legislative procedure (third reading)

(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 strikeout. 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>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION</td>
</tr>
<tr>
<td>EXPLANATORY STATEMENT</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 Article 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 Economic and Social Committee of 2 March 2021,[3]
– having regard to the opinion of the European Central Bank[4],
– 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 (A9-0000/2021),

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

Proposal for a directive
Title


Amendment 2
Proposal for a directive
Recital 4

Text proposed by the Commission

(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 accordance with the requirements laid down in Regulation (EU) 2021/xx [DORA].

Amendment

(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 accordance with the requirements laid down in Regulation (EU) 2021/xx [DORA]. Furthermore, ICT risk is only implicitly included in the supervisory review and evaluation process (SREP) performed by competent authorities as part of operational risk and the criteria for its assessment are currently defined in 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*. 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.


Amendment 3
Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission

(4a) Digital operational resilience is an essential condition to preserve the critical functions and core business lines of an institution in the event of its resolution and thereby avoid disruption to the real economy and to the financial system. Major ICT-related incidents and ICT vulnerabilities can hamper the capacity of an institution to continue operating and can jeopardise the 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. It is therefore indispensable that resolution authorities have access to timely and accurate information on ICT risks as well as on ICT service contracts in order to identify and ensure the continuance of critical functions. In order to be aligned, and ensure consistency, with the objectives of the Union framework for bank recovery and resolution, Directive 2014/59/EU should be amended to clarify that the information on ICT risks and on ICT service contracts should be taken into account in the context of resolution planning and the assessment of institutions’ resolvability. Moreover, resolution authorities should be explicitly included among the authorities that receive notifications of major ICT-related incident reporting for the entities under their remit, in accordance with the DORA Regulation.

Amendment 4

Proposal for a directive
Recital 4 b (new)

Text proposed by the Commission

(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 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 Basel Progress Report of April 2020 and the ECB Report on the Thematic Review of May 2018 on effective risk data aggregation and risk reporting 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 ESRB, should produce a report to assess how the BCBS 239 principles interact with the provisions of the DORA Regulation and if appropriate how those principles should be incorporated in Union law.

Or. en

Amendment 5
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”). 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. In order to ensure a consistent application across jurisdictions, in line with the approach ‘same business, same risk, same rules’ and to avoid creating regulatory arbitrage, the criteria for the qualification of crypto-assets as financial instruments within the meaning of point (15) of Article 4(1) of Directive 2014/65/EU, should be further specified by means of regulatory technical standards issued by the European Supervisory Authority (European Securities and Markets Authority) (ESMA), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council*.


Or. en

Amendment 6

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

Amendment

(7) 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 a DLT multilateral trading facility, operated by an investment firm or a market operator
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.

authorised under Directive 2014/65/EU (MiFID), that has been granted a specific permission under Regulation (EU) 2021/xx of the European Parliament and of the Council\(^2\) [Proposal for a regulation on a pilot regime on DLT market infrastructure]. 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 temporary legal framework should be subject to all the requirements applicable to a multilateral trading facility under Directive 2014/65/EU, except if such a facility were to be granted an exemption by its national competent authority from the obligation of intermediation set out in Directive 2014/65/EU in accordance with this Directive. 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. That requirement can amount to a regulatory barrier to the development of a multilateral trading facility for transferable securities issued on a DLT. 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 the obligation of intermediation, allowing retail investors direct access to DLT multilateral trading facilities, provided that adequate safeguards are in place in terms of investor protection.

Or. en
Justification

Clarifies that the exemption from MiFID granted to the DLT multilateral trading facility only concerns the derogation from the obligation of intermediation.

Amendment 7
Proposal for a directive
Recital 8

Text proposed by the Commission

(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\(^7\) [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 it can provide retail investors with easy access to the trading venue, provided that adequate safeguards are in place in terms of investor...
**Amendment 8**

**Proposal for a directive**

**Recital 9**

*Text proposed by the Commission*

(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 them with 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.

*Amendment*

(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 them with Regulation (EU) 2021/xx [DORA]. Furthermore, the incident notification rules in that Directive **cover in substance the same category of risks as those addressed by the major ICT-related incident reporting rules under DORA**. In order to strengthen supervisory effectiveness and avoid unnecessary complexity and duplication of reporting requirements, it is therefore appropriate to create a single incident reporting mechanism for payment service providers. As a consequence, the incident notification rules in Directive (EU) 2015/2366 should be replaced by the incident notifications that Regulation (EU) 2021/xx[DORA] fully harmonises. **With a view to ensuring that all major operational or security incidents are covered, the term ‘major ICT-related incidents’ should be clearly defined in DORA, also taking into account EBA’s guidelines on major incident reporting under Directive (EU) 2015/2366.**

Or. en
Amendment 9

Proposal for a directive
Recital 10 a (new)

Text proposed by the Commission

(10a) Building a high level of digital operational resilience is crucial in order to strengthen the ability of financial institutions to combat money laundering and terrorist financing, especially in light of the increasing and emerging risks in that area, opened up by the COVID-19 pandemic. The pandemic has put strong pressure on the digital operational resilience capabilities of financial institutions and of ICT third-party service providers. That, in turn, has created an environment in which criminals can exploit weaknesses and gaps in institutions’ systems and controls put in place to fight financial crime. The framework established by Regulation [DORA] to strengthen the digital operational resilience of financial entities should therefore contribute to enhancing their ability to combat money laundering and terrorist financing. In order to ensure that the digital operational resilience dimension is properly addressed, Directive (EU) 2015/849 should be amended to explicitly include, in respect of obliged entities that fall within the scope of the DORA Regulation, the DORA requirements as part of the policies, controls and procedures put in place by those obliged entities in order to mitigate and manage effectively the risks of money laundering and terrorist financing.

Or. en
Amendment 10
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 and accounting procedures and control and safeguard arrangements for electronic data processing, including 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], 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;

Or. en

Justification

The references to the DORA Regulation across the different financial services directives are amended to ensure alignment with the formulation of 'network and information systems' used to define the subject matter of the DORA Regulation and to cover all applicable requirements.

Amendment 11
Proposal for a directive
Article 3 – paragraph 1 – point 1
Directive 2009/138/EC
Article 41 – paragraph 4

Text proposed by the Commission

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].

Amendment

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 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. […]).

Amendment 12

Proposal for a directive
Article 4 – paragraph 1
Directive 2011/61/EC
Article 18 – paragraph 1 – subparagraph 2

Text proposed by the Commission

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.

Amendment

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
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.

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

Amendment 13
Proposal for a directive
Article 5 – paragraph -1 (new)
Directive 2013/36/EU
Article 74 – paragraph 1 – subparagraph 1

Present text

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, and remuneration policies and practices that are consistent with and promote sound and effective risk management.

Amendment

-1. In Article 74, 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 as well as network and information systems 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.’
Amendment 14

Proposal for a directive
Article 5 – paragraph -1 a (new)
Directive 2013/36/EU
Article 85 – paragraph 1

Present text

1. Competent authorities shall ensure that institutions implement policies and processes to evaluate and manage the exposures to operational risk, including model risk and risks resulting from outsourcing, and to cover low-frequency high-severity events. Institutions shall articulate what constitutes operational risk for the purposes of those policies and procedures.

Amendment

-1a. In Article 85 of Directive 2013/36/EU, paragraph 1 is replaced by the following:

‘1. Competent authorities shall ensure that institutions implement policies and processes to identify, evaluate and manage the exposures to operational risk, including risks resulting from outsourcing and sub-outsourcing and ICT risk in accordance with 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 articulate the main sources of operational risk for the purposes of those policies and procedures.’

Amendment 15

Proposal for a directive
Article 5 – paragraph 1
Directive 2013/36/EU
Article 85 – paragraph 2

Text proposed by the Commission

2. Competent authorities shall ensure that institutions have adequate contingency

Amendment

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. […]).’

Amendment 16

Proposal for a directive
Article 5 – paragraph 1 a (new)
Directive 2013/36/EU
Article 97 – paragraph 1 – point a a (new)

Text proposed by the Commission

Amendment

1a. In Article 97(1), the following point is inserted:

‘(aa) 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];’

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

Amendment 17

Proposal for a directive
Article 5 – paragraph 1 b (new)
Directive 2013/36/EU
Article 97 – paragraph 2

Present text

2. The scope of the review and evaluation referred to in paragraph 1 shall cover all requirements of this Directive and of Regulation (EU) No 575/2013.

Amendment

Ib. In Article 97, paragraph 2 is replaced by the following:

‘2. The scope of the review and evaluation referred to in paragraph 1 shall cover all 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].’

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

Or. en


Amendment 18

Proposal for a directive
Article 5 – paragraph 1 c (new)
Directive 2013/36/EU
Article 98 – paragraph 1 – point j a (new)

Text proposed by the Commission

1c. In Article 98(1) the following point is added:

‘(ja) major ICT-related incident reports drawn up by institutions in accordance with Chapter III of Regulation (EU)2021/xx of the European Parliament and of the Council [DORA];’

Or. en

Amendment 19

Proposal for a directive

Article 5 – paragraph 1 d (new)
Directive 2013/36/EU
Article 98 – paragraph 1 – point j b (new)

Text proposed by the Commission

Amendment

Id. In Article 98(1) the following point is added:

‘(jb) the results of digital operational resilience tests carried out by institutions in accordance with Chapter IV of Regulation (EU)2021/xx of the European Parliament and of the Council [DORA].’

Or. en


Amendment 20

Proposal for a directive

Article 5 – paragraph 1 e (new)
Directive 2013/36/EU
Article 107 – paragraph 3

Present text

Amendment

1e. Article 107(3) is replaced by the following:

‘3. EBA shall issue guidelines addressed to the competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010 to further specify, in a manner that is appropriate to the size, the structure and the internal organisation of institutions and the nature, scope and complexity of their activities, the common procedures and methodologies for the supervisory review and evaluation process referred to in paragraph 1 of this Article and in Article

and in Article 97 and for the assessment of the organisation and treatment of the risks referred to in Articles 76 to 87, in particular relating to concentration risk in accordance with Article 81.

and in Article 97 and for the assessment of the organisation and treatment of the risks referred to in Articles 76 to 87, in particular relating to concentration risk in accordance with Article 81 and to operational risk in accordance with Article 85, taking into account the provisions on ICT risk management laid down in Regulation (EU) 2021/xx [DORA].’


Amendment 21

Proposal for a directive

Article 5 a (new)

Text proposed by the Commission

Amendment

Article 5a

Amendments to Directive 2014/59/EU

Directive 2014/59/EU is amended as follows:

(1) in Article 10:

(a) point (c) of paragraph 7 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) point (q) of paragraph 7 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
(c) the following subparagraph is added in paragraph 9:

‘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) in the Annex:

(a) point (16) of Section A 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 and ICT services in accordance with Regulation (EU) 2021/xx [DORA];’;

(b) point (14) of Section B 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 intra-group or third-party ICT service providers;’;

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

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

(d) point (4) of Section C 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) the following point is inserted in Section C:
‘(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].’.

Or. en


Justification

Amendments to Bank Recovery and Resolution Directive (BRRD) necessary to include network and information systems that support critical functions in resolution planning (Art. 10) and to integrate information related to major incident reports and results of digital resilience tests performed in accordance with DORA as well as ICT services contracts in the list of information in the Annex resolution authorities should consider for the purpose of resolution planning and the resolvability assessment.

Amendment 22

Proposal for a directive
Article 6 – paragraph 1 – point 1 a (new)
Directive 2014/65/EU
Article 4 – paragraph 2 a (new)

Text proposed by the Commission

(1a) In Article 4, the following paragraph is added:
‘2a. ESMA shall develop draft regulatory technical standards to specify, for the purposes of point 15 of paragraph 1, the criteria and conditions to establish when an instrument qualifies as a financial instrument, applying the principle of technological neutrality. ESMA shall submit those draft regulatory technical standards to the Commission by
[12 months after the date of entry into force of this amending directive].

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.’

Or. en

Amendment 23
Proposal for a directive
Article 6 – paragraph 1 – point 5 – point a
Directive 2014/65/EU
Article 47 – paragraph 1 – point b

Text proposed by the Commission

(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.

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

Amendment

(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 all significant risks to its operation, and to put in place effective measures to mitigate those risks.

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

Or. en


Amendment 24
Proposal for a directive
Article 6 – paragraph 1 – point 6 – point a
Directive 2014/65/EU
Article 48 – paragraph 1
1. Member States shall require a regulated market to build its operational resilience in accordance with the requirements laid down in \textit{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.

Or. en


\textbf{Amendment 25}

\textbf{Proposal for a directive}

\textbf{Article 7 – paragraph 1 – point -1 (new)}

Directive (EU) 2015/2366

Article 5 – paragraph 1 – point e

\textit{Present text}

(e) a description of the applicant’s governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, which demonstrates that those governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;

\textit{Amendment}

(-1) \textit{In Article 5(1), 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;’

_________

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

Or. en


Amendment 26

Proposal for a directive
Article 7 – paragraph 1 – point -1 a (new)
Directive (EU) 2015/2366
Article 5 – paragraph 1 – point f

<table>
<thead>
<tr>
<th>Present text</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incidents reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96;</td>
<td>(-1a) In Article 5(1), point (f) is replaced by the following:</td>
</tr>
<tr>
<td></td>
<td>‘(f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incidents 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];’</td>
</tr>
</tbody>
</table>

_________________________________________________________________________

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

Or. en


Justification

Two parallel reporting frameworks under DORA and PSD2 may create complexity and overlaps, which would in turn reduce the effectiveness of supervision. It would therefore be appropriate that incident reporting rules of PSD2 are fully aligned with the incident reporting rules harmonised by DORA Regulation.
Amendment 27

Proposal for a directive
Article 7 – paragraph 1 – point b (new)
Directive 2015/2366/EU
Article 5 – paragraph 1 – point h

Present text
(h) a description of business continuity arrangements including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans;

Amendment
(-1b) In Article 5(1), 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];’


Amendment 28

Proposal for a directive
Article 7 – paragraph 1 – point a (new)
Directive (EU) 2015/2366
Article 20 – paragraph 1

Present text
1. Member States shall ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of this Directive are complied with.

Amendment
(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, 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* [DORA] are complied with.

______________
Amendment 29

Proposal for a directive
Article 7 – paragraph 1 – point 2 – point a
Directive (EU) 2015/2366
Article 95 – paragraph 1

Text proposed by the Commission

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].

Amendment

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 and communication technology in accordance with Chapters II and III of Regulation (EU) 2021/xx [DORA].

Or. en

Amendment 30

Proposal for a directive
Article 7 – paragraph 1 – point 2 – point c
Directive (EU) 2015/2366
Article 95 – paragraph 5

Text proposed by the Commission

(c) paragraph 5 is replaced by the following:

Amendment

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.

Justification
To maintain the current text which includes, where relevant, the European Union Agency for Network and Information Security

Amendment 31
Proposal for a directive
Article 7 – paragraph 1 – point 3 – point a
Directive (EU) 2015/2366
Article 96 – paragraph 1

Text proposed by the Commission
(a) paragraph 1 is replaced by the following:

Amendment
(a) in paragraph 1, the first subparagraph is replaced by the following:

Amendment 32
Proposal for a directive
Article 7 – paragraph 1 – point 3 – point a
Directive (EU) 2015/2366
Article 96 – paragraph 1

Text proposed by the Commission
1. In case of a major operational or security 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.

Amendment
1. In case of a major operational or security incident, the payment service provider shall report to the relevant competent authority in accordance with Chapter III of Regulation (EU)2021/xx of the European Parliament and of the Council * [DORA].
**Justification**

Since there is no clear delineation between ICT-related and other kind of operational or security incidents, it would be appropriate to create a single set of incident reporting rules for payment service providers fully harmonised under DORA rather than a dual system for incident reporting, which may create overlaps and unnecessary complexity.

**Amendment 33**

**Proposal for a directive**

**Article 7 – paragraph 1 – point 3 – point a a (new)**

Directive (EU) 2015/2366

Article 96 – paragraph 1 – subparagraph 2

**Present text**

Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

**Amendment**

Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident, in accordance with Article 17 of Regulation (EU) xx/20xx[DORA].


**Amendment 34**

**Proposal for a directive**

**Article 7 – paragraph 1 – point 3 – point a b (new)**

Directive 2015/2366/EU

Article 96 – paragraph 2 – subparagraph 1

**Present text**

**Amendment**

Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of measures that they can take to mitigate the adverse effects of the incident, in accordance with Article 17 of Regulation (EU) xx/20xx[DORA].
Upon receipt of the notification referred to in paragraph 1, the competent authority of the home Member State shall, without undue delay, provide the relevant details of the incident to EBA and to the ECB. That competent authority shall, after assessing the relevance of the incident to relevant authorities of that Member State, notify them accordingly.

‘In accordance with Article 17 of Regulation (EU) xx/20xx [DORA], upon receipt of the notification referred to in paragraph 1, the relevant competent authority shall, without undue delay, provide the details of the incident to EBA and to the ECB.’


Justification

The PSD2 incident reporting is replaced by the incident reporting rules under DORA.

Amendment 35
Proposal for a directive
Article 7 a (new)

Text proposed by the Commission

Amendment

Article 7a

Amendment to Directive (EU) 2015/849

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

‘(ba) 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].’

Justification

Targeted amendment to the Anti-money Laundering Directive aimed at clarifying that the measures related to ICT risks put in place by those obliged entities covered under the DORA
Regulation are consistent with that Regulation, where applicable. This amendment does not aim to enlarge the scope of DORA to other obliged entities that are not financial entities.

Amendment 36

Proposal for a directive
Article 8 – paragraph 1
Directive (EU) 2016/2341
Article 21 – paragraph 5

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>To that end, IORPs shall employ appropriate and proportionate systems, resources and procedures and shall set up <strong>ICT systems and tools</strong> and manage them in accordance with <strong>Article 6 of Regulation (EU) 2021/xx of the European Parliament and of the Council</strong> [DORA].</td>
<td>To that end, IORPs shall employ appropriate and proportionate systems, resources and procedures and shall set up <strong>network and information systems</strong> and manage them in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council [DORA].</td>
</tr>
</tbody>
</table>
EXPLANATORY STATEMENT

This legislative proposal is part of the Digital Finance Package, which comprises a proposal for a Regulation on markets in crypto-assets, a proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT) and a proposal for a Regulation on digital operational resilience for the financial sector.

The purpose of this proposal is twofold: on the one hand, it introduces targeted changes to existing EU financial services directives in order to align them with the requirements on network and information systems and ICT risk management and reporting laid down in the DORA Regulation and clarify certain provisions to ensure ICT risks are fully addressed.

On the other hand, it introduces targeted changes to the MIFID Directive to provide legal certainty as regards the definition of crypto assets and to establish a temporary exemption allowing natural persons to participate to the pilot regime for a DLT Multilateral Trading Facility, under certain conditions.

The Rapporteur supports the overall approach followed by the Commission but believes further changes and clarifications to existing financial services directives are needed to increase legal clarity and consistency.

In relation to the amendments related to the DORA Regulation, the changes proposed by the Rapporteur aim to address the following issues:

• Amendment to Directive 2013/36/EU (CRD): ICT risk are covered only implicitly in the CRD as part of operational risk and are currently addressed in the supervisory review and evaluation process (SREP) on the basis of EBA guidelines. The relevant CRD provisions could therefore be clarified as to ensure that ICT risk is explicitly addressed together with outsourcing and sub-outsourcing risks as part of the operational risk. Moreover, the provisions on the SREP should be amended to explicitly include ICT risk and ensure that major incident report and the results of the digital operational resilience tests performed in accordance with DORA are taken into account as part of the assessment.

• Amendment to Directive 2014/59/EU (BBRD): ICT risks and vulnerabilities to digital operational resilience may impact the network and information systems that support critical functions of the banks and undermine the resolution objectives. Information related to major incidents reports and the results of digital operational resilience tests should therefore be fully taken into account by resolution authorities in the context of the resolution planning and resolvability assessment in relation to the banks under the remit. A mandate should be given to EBA to review and update the regulatory standards in light of the new framework. This would be complementary to possible changes to the DORA Regulation, inter alia, to include resolution authorities among the recipients of incident notifications.

• Amendment to PSD2 Directive: the Commission proposal maintains the existing incident reporting rules under PSD2 for operational incidents that are non-ICT related, which would create a parallel mechanism of reporting for payment service providers next to the one introduced under the DORA Regulation for ICT-related incidents. However, since operational or security incidents are in fact mostly related to ICT and it may be difficult to distinguish between ICT and non-ICT incidents, the Rapporteur believes that such dual system of reporting may create complexity and overlaps and in turn reduce the effectiveness of supervision. It would therefore be appropriate that the incident reporting provisions under PSD2 are fully aligned with the incident reporting rules harmonised by DORA, with the aim
to establish a single incident reporting mechanism for payment service providers covering all operational or security incidents. A single channel of incident reporting may also require an adjustment of the definition of “major ICT-related incident” in the DORA Regulation to ensure that all major operational or security incidents are covered. Moreover, the scope of DORA should also be revised to ensure that all payment services providers are covered for the purpose of the incident reporting.

- Amendment to AML Directive: given the crucial role of network and information systems for the fight against money laundering and the increasing ICT-related risks and vulnerabilities opened up by the COVID-19 pandemic in this context, it would be appropriate to introduce a targeted amendment to already clarify, without waiting for a future proposal on the AML framework, that the internal controls and policies put in place by those obliged entities covered under the DORA Regulation should be consistent with that Regulation. This amendment does not aim to enlarge the scope of DORA to other obliged entities.

- Amendments to the terminology: general references to the DORA Regulation are amended in order to ensure they are consistent and aligned with the relevant subject matter and across financial services legislation. In general, the term ‘network and information systems’ as defined in the NIS Directive and indicated as the subject matter of the DORA Regulation is preferred to other formulations related to ICT systems which are not clearly defined in the DORA Regulation.

In relation to the definition of crypto-assets, the Rapporteur welcomes the amendment to the MIFID Directive proposed by the Commission, which clarifies that the definition of financial instrument may also include instrument based on distributed ledger technology (DLT) when they can be qualified as financial instruments. However, in order to improve legal certainty and create a level playing field among jurisdictions, the criteria and condition for the qualification of a crypto-asset as financial instrument should be further specified by technical standards to be developed by ESMA.

Finally, in relation to the MIFID amendments linked to the DLT multilateral trading facility, the Rapporteur agrees in principle that retail investors should be allowed to participate to the pilot regime. However, the Rapporteur is of the opinion that the pilot regime should ensure high standards of protection for retail investors and the inclusion of additional safeguards in the MIFID provisions may be considered at a later stage, taking into account the developments in the dedicated Regulation. Furthermore, it should be clarified that the only exemption from MIFID provisions in relation to the DLT pilot regime concerns the derogation from the obligation of intermediation, while other provisions would still apply.