Council of the European Union

Brussels, 4 June 2021
(OR. en)

9530/21

Interinstitutional Files:
2020/0266 (COD)
2020/0268 (COD)

EF 189
ECOFIN 576
TELECOM 246
CYBER 169
CODEC 839

COVER NOTE

From:	Ms Christine LAGARDE, President of the European Central Bank
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
Subject:	Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/20141; and on a proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341

Delegations will find attached the opinion mentioned above, and its technical working document.

Encl.

EUROPEAN CENTRAL BANK
EUROSYSTEM

OPINION OF THE EUROPEAN CENTRAL BANK

of 4 June 2021

on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector

(CON/2021/20)

Introduction and legal basis

On 22, 23 and 29 December 2020 the European Central Bank (ECB) received requests from the Council of the European Union and the European Parliament, respectively, for an opinion on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014[1] (hereinafter the 'proposed regulation') and a proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341[2] (hereinafter the 'proposed amending directive', together with the 'proposed regulation', the 'proposed acts').

The ECB's competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union, as the proposed acts contain provisions falling within the ECB's fields of competence, in particular, the definition and implementation of monetary policy, the promotion of the smooth operation of payment systems, the contribution to the smooth conduct of policies pursued by competent authorities relating to the stability of the financial market system, and the ECB's tasks concerning the prudential supervision of credit institutions pursuant to the first and fourth indents of Article 127(2), Article 127(5) and Article 127(6) of the Treaty. In accordance with the first sentence of Article 17.5 of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

1. General observations

1.1 The ECB welcomes the proposed regulation, which aims to enhance the cyber security and operational resilience of the financial sector. In particular, the ECB welcomes the aim of the proposed regulation to remove obstacles to, and improve the establishment and functioning of, the internal market for financial services by harmonising the rules applicable in the area of information and communication technology (ICT) risk management, reporting, testing and ICT third-party risk. Furthermore, the ECB welcomes the aim of the proposed regulation to streamline and harmonise any overlapping regulatory requirements or supervisory expectations to which financial entities are currently subject under Union law.

1 COM(2020) 595 final.
2 COM(2020) 596 final.

1.2 The ECB understands that the proposed regulation represents, in relation to financial entities identified as operators of essential services[3], sector specific legislation (*lex specialis*) in accordance with the meaning as set out in Article 1(7) of Directive (EU) 2016/1148 of the European Parliament and of the Council[4] (hereinafter the 'NIS Directive'); this implies that the requirements under the proposed regulation would, in principle, prevail over the NIS Directive. In practice, financial entities identified as operators of essential services[5] would, inter alia, report incidents in accordance with the proposed regulation rather than the NIS Directive. While the ECB welcomes the reduction of potential overlapping requirements for financial entities in the field of incident reporting, further consideration should be given to the interplay between the proposed regulation and the NIS Directive. For example, under the proposed regulation an ICT third-party service provider[6] could be subject to recommendations issued by the lead overseer[7]. At the same time, the very same ICT third-party service provider may be classified as an operator of essential services under the NIS Directive and be subject to binding instructions issued by the competent authority[8]. In such case, the ICT third-party service provider could be subject to conflicting recommendations issued under the proposed regulation and binding instructions issued under the NIS Directive. The ECB suggests that the Union legislative bodies reflect further on potential inconsistencies between the proposed regulation and the NIS Directive that may hamper the harmonisation and reduction of overlapping and conflicting requirements for financial entities.

1.3 The ECB also understands that under the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148[9] (hereinafter the 'proposed NIS2 directive'), 'near misses'[10] will be subject to reporting obligations[11]. While Recital (39) of the proposed NIS2 directive refers to the meaning of the term 'near misses', it is unclear whether the intention is to require that near misses be reported by the financial entities listed in Article 2 of the proposed regulation. In this regard, and also taking into account that near misses can only be identified as such after they have occurred, the ECB would welcome receiving notification of significant near-misses in a timely manner, as is currently the case for cyber incidents. The ECB suggests that there should be greater coordination between the proposed regulation and the proposed NIS2 directive to clarify the exact scope of reporting to which any given financial entity may be subject under these two distinct but connected pieces of Union legislation. At the same time, 'near misses' would need to be defined and provisions clarifying their significance would need to be developed.

---

3 See Article 1(2) of the proposed regulation.

4 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

5 See Article 5 of the NIS Directive.

6 See Article 3(15) of the proposed regulation.

7 See Article 31(1)(d) of the proposed regulation.

8 See Article 15(3) of the NIS Directive.

9 COM(2020) 823 final.

10 Events that could potentially have caused harm, but were successfully prevented from fully transpiring; see Recital (39) of the NIS2 Directive.

11 See Article 11 of the NIS2 Directive.

1.4 The ECB welcomes incentivising financial entities to share on a voluntary basis cyber threat intelligence information amongst each other to enhance and bolster their cyber resilience postures. The ECB itself has assisted with the market-driven Cyber threat Intelligence Information Sharing Initiative (CIISI-EU) and has made available the blueprints for anyone to build and foster such an initiative[12].

1.5 The ECB supports cooperation between the competent authorities for the purposes of the proposed regulation, the European Supervisory Authorities (ESAs), and the Computer Security Incident Response Teams (CSIRTS)[13]. It is essential to exchange information in order to ensure the operational resilience of the Union, as information sharing and cooperation among authorities can contribute to the prevention of cyber-attacks and help reduce the spread of ICT threats. A common understanding of ICT-related risks should be promoted and assessing such risks in a consistent manner should be ensured across the Union. It is of utmost importance that information be shared with the single point of contact[14] and the national CSIRTS by competent authorities[15] only when there are clearly established classification and information sharing mechanisms, coupled with adequate safeguards to ensure confidentiality.

1.6 Finally, the ECB would welcome the introduction under the proposed regulation of rules on personal data and data retention. The length of the retention period should take into account the investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight or supervisory plans that the competent authorities may have to carry out as part of their respective obligations and duties under the proposed regulation. In this respect, a 15-year retention period would be adequate. This data retention period could be shortened or extended, as specific instances require. In this respect, the ECB suggests that the Union legislative bodies, in their formulation of the relevant provision on personal data and data retention, also take into account the data minimisation principle, as well as further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[16].

2. Specific observations on oversight and securities clearing and settlement

2.1 *ESCB and Eurosystem oversight competences*

2.1.1 Closely linked to its basic monetary policy tasks, the Treaty and the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the Statute of the ESCB) provide for the Eurosystem's conduct of oversight over clearing and payment systems. Pursuant to the fourth indent of Article 127(2) of the Treaty, as mirrored in Article 3.1 of the Statute of the ESCB, one of the basic tasks to be carried out through the European System of Central Banks (ESCB) is to promote the smooth operation of payment systems. In the performance of this basic task, the ECB and the

12 Cyber threat Intelligence Information Sharing Initiative (CIISI-EU) available at the ECB's website www.ecb.europa.eu.

13 See Article 42 of the proposed regulation.

14 See Article 8(3) of the NIS Directive.

15 See also Articles 11, 26 and 27 of the NIS2 Directive.

16 See Articles 4(b) and 13 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payments systems within the Union and with other countries[17]. Pursuant to its oversight role, the ECB adopted Regulation (EU) No 795/2014 of the European Central Bank (ECB/2014/28) (hereinafter the 'SIPS Regulation')[18]. The SIPS Regulation implements, in prescriptive form, the Principles for financial market infrastructures of April 2012 issued by the Committee on Payment and Settlement Systems and the International Organisation of Securities Commissions[19], which are legally binding and cover both large-value and retail payment systems of systemic importance, operated either by a Eurosystem central bank or a private entity. The Eurosystem oversight policy framework[20] identifies payment instruments as an 'integral part of payment systems' and thus includes these within the scope of its oversight. The oversight framework for payment instruments is currently under review[21]. Under that framework, a payment instrument (e.g. a card, credit transfer, direct debit, e-money transfer and digital payment token[22]) is defined as a personalised device (or a set of devices) and/or set of procedures agreed between the payment service user and the payment service provider used in order to initiate a transfer of value[23].

2.1.2 In the light of the above, the ECB welcomes the exclusion from the proposed regulation's scope article of system operators as defined in point (p) of Article 2 of Directive 98/26/EC of the European Parliament and of the Council[24], payment systems (including those operated by central banks), payment schemes and payment arrangements in view of the application of the above-referenced oversight frameworks. For these reasons, the ESCB's competences under the Treaty and the Eurosystem's competences under the SIPS Regulation should be clearly spelled out in the recitals of the proposed regulation.

2.1.3 By the same token, the ECB welcomes the exclusion from the application of the oversight framework set out in the proposed regulation of ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty[25]. In this respect, the ECB would like to stress that ESCB central banks acting in their

17 See Article 22 of the Statute of the ESCB.

18 Regulation (EU) No 795/2014 of the European Central Bank of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, p. 16).

19 Available on the Bank for International Settlements' website at www.bis.org.

20 Eurosystem oversight policy framework, Revised version (July 2016) available on the ECB's website at www.ecb.europa.eu.

21 See the revised and consolidated Eurosystem oversight framework for electronic payment instruments, schemes and arrangements of October 2020 (PISA framework), available on the ECB's website at www.ecb.europa.eu.

22 A digital payment token is a digital representation of value backed by claims or assets recorded elsewhere and enabling the transfer of value between end users. Depending on the underlying design, digital payment tokens can foresee a transfer of value without necessarily involving a central third-party and/or using payment accounts.

23 'Transfer of value' "The act, initiated by the payer or on the payer's behalf or by the payee, of transferring funds or digital payment tokens, or placing or withdrawing cash on/from a user account, irrespective of any underlying obligations between the payer and the payee. The transfer can involve a single or multiple payment service providers." This definition of 'transfer of value' under the PISA framework departs from the definition of a transfer of 'funds' under Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35). A 'transfer of value' in the context of a 'payment instrument' as defined in that Directive can only refer to a transfer of 'funds'. Under that Directive, 'funds' do not include digital payment tokens unless the tokens can be classified as electronic money (or more hypothetically as scriptural money).

24 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.6.1998, p. 45).

25 See Article 28(5) of the proposed regulation.

monetary capacities[26] and the Eurosystem when providing services via TARGET2, TARGET2-Securites (T2S)[27] and TARGET Instant Payment Settlement (TIPS)[28] are not subject to the scope article of the proposed regulation, nor can they be deemed ICT third-party service providers and thus potentially classified as critical ICT third-party service providers for the purposes of the proposed regulation. The Eurosystem oversees T2S in connection with its mandate to ensure efficient and sound clearing and payment systems. Furthermore, ESMA has clarified that T2S is not a critical service provider[29] within the meaning of Regulation (EU) No 909/2014 of the European Parliament and of the Council[30] (hereinafter the 'CSD Regulation'). As a result, T2S's organisational and operational safety, efficiency and resilience are ensured through the applicable legal, regulatory and operational framework and agreed governance arrangements or T2S, as opposed to via the CSD Regulation.

2.1.4 In addition, the Eurosystem's oversight policy framework[31] covers critical service providers such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a limited liability cooperative company established in Belgium, which provides secure messaging services internationally. The Nationale Bank van België/Banque Nationale de Belgique acts as lead overseer of SWIFT, and conducts, on the basis of a cooperative oversight arrangement, oversight in respect of SWIFT, in cooperation with the other G10 central banks, including the ECB. The G10 overseers recognise that the main focus of oversight is SWIFT's operational risk, as this is considered to be the primary risk category through which SWIFT could pose a systemic risk to the financial system in the Union. In this regard, the SWIFT Cooperative Oversight Group has developed a specific set of principles and high-level expectations that apply to SWIFT, such as risk identification and management, information security, reliability and resilience, technology planning and communication with users. The G10 overseers expect SWIFT to adhere to the Committee on Payment and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) Guidance on cyber resilience[32] as well as other international standards on ICT security which, when taken together, exceed the requirements set out in the proposed regulation.

---

26 See paragraph 1.3 of Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (CON/2021/4). All ECB Opinions are published in EUR-Lex.

27 See Annex IIa to Guideline ECB/2012/27 of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 30, 30.1.2013, p. 1). Guideline ECB/2012/13 of the European Central Bank of 18 July 2012 on TARGET2-Securities (OJ L 215, 11.8.2012, p. 19); Decision ECB/2011/20 of the European Central Bank of 16 November 2011 establishing detailed rules and procedures for implementing the eligibility criteria for central securities depositories to access TARGET2-Securities services (OJ L 319, 2.12.2011, p. 117). See also the T2S Framework Agreement and the Collective Agreement.

28 See Annex IIb to Guideline ECB/2012/27.

29 See Article 30(5) of Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1) and Article 68 of Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (OJ L 65, 10.3.2017, p. 48).

30 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

31 Eurosystem oversight policy framework, Revised version (July 2016) available on the ECB's website at www.ecb.europa.eu.

32 Available on the Bank for International Settlements' website at www.bis.org.

2.1.5 One cannot be certain that SWIFT and perhaps other service providers subject to the Eurosystem oversight policy framework, could become subject to the proposed regulation as ICT third-party service providers if they were to provide services not covered under Article 127(2) of the Treaty. The ECB therefore strongly welcomes that service providers already subject to the Eurosystem oversight policy framework, including but not limited to SWIFT, be excluded from the scope of application of the oversight framework set out under the proposed regulation.

2.2 *ESCB competences in the area of securities settlement*

2.2.1 Central securities depositories (CSDs) are financial market infrastructures (FMIs) that are strictly regulated and supervised by different authorities pursuant to the CSD Regulation, which sets out requirements pertaining to the settlement of financial instruments as well as rules on the organisation and conduct of CSDs. Furthermore, CSDs should take note of the CPMI-IOSCO Guidance on cyber resilience, which has been operationalised by the Cyber resilience oversight expectations for financial market infrastructures (December 2018)[33] . In addition to the supervisory competences entrusted to national competent authorities (NCAs) under the CSD Regulation, the members of the ESCB act as 'relevant authorities', in their capacity as overseers of securities settlement systems operated by CSDs, central banks issuing the most relevant currencies in which settlement takes place and central banks in whose books the cash leg of transactions is settled[34]. In this regard, recital 8 of the CSD Regulation states that the Regulation should apply without prejudice to the responsibilities of the ECB and the national central banks to ensure efficient and sound clearing systems and payment systems within the Union and other countries. Recital 8 also states that the CSD Regulation should not prevent the members of the ESCB from accessing information relevant to the performance of their duties[35], including the oversight of CSDs and other FMIs[36].

2.2.2 In addition, the members of the ESCB often act as settlement agents for the cash leg of securities transactions and the Eurosystem offers settlement services via T2S to CSDs. The Eurosystem's oversight of T2S is related to its mandate to ensure efficient and sound clearing and payment systems, while competent and relevant authorities of CSDs aim to ensure their smooth functioning, the safety and efficiency of settlement and the proper functioning of financial markets in their respective jurisdictions.

2.2.3 Under the proposed regulation[37] ESCB central banks are not involved in the development of technical standards as regards the specification of ICT risks. Similarly, under the proposed regulation[38] the relevant authorities are not informed of any ICT related incidents. ESCB central bank should keep the same level of involvement as currently provided under the CSD Regulation and the

33 Available on the ECB's website at www.ecb.europa.eu.

34 See Article 12 of Regulation (EU) No 909/2014.

35 See also Article 13, and Articles 17(4) and 22(6) of Regulation (EU) No 909/2014.

36 See paragraph 7.3 of Opinion of the European Central Bank of 6 April 2017 on the identification of critical infrastructures for the purpose of information technology security (CON/2017/10); paragraph 7.2 of Opinion of the European Central Bank of 8 November 2018 on designation of essential services and operators of essential services for the purpose of network and information systems security (CON/2018/47); paragraph 3.5.2 of Opinion of the European Central Bank of 2 May 2019 on the security of network and information systems (CON/2019/17); and paragraph 3.5.2 of Opinion of the European Central Bank of 11 November 2019 on the security of network and information systems (CON/2019/38).

37 See Article 54(5) of the proposed regulation and Article 45(7) of Regulation (EU) No 909/2014.

38 See Article 54(4) of the proposed regulation and Article 45(6) of Regulation (EU) No 909/2014.

relevant authorities should be notified of ICT related incidents. The Eurosystem is the relevant authority for all euro area CSDs and for several other EU CSDs. ESCB central banks would need to be informed about ICT-related incidents that are relevant to the performance of their duties, including the oversight of CSDs and other FMIs. The risks to which CSDs are exposed, including ICT risks, have the potential to threaten the sound functioning of CSDs. Therefore, ICT risks are of importance to relevant authorities, which should be provided with a full and detailed overview of these risks in order to assess them and influence the CSDs' risk management approach. The proposed regulation should not provide for less restrictive requirements as regards ICT risks when compared to those provided under the CSD Regulation and current related regulatory technical standards.

2.2.4 In addition, the Union legislative bodies should clarify the interplay between the proposed regulation[39] and the regulatory technical standards supplementing the CSD Regulation. In particular, it is not clear whether a CSD is to be exempted from the obligation of having its own secondary site where its ICT third-party service provider maintains such a site[40]. Should a CSD be exempt from this obligation to maintain a secondary site, it is unclear what legal value this requirement would have. By the same token, the proposed regulation[41] refers to a recovery time objective and recovery point objectives for each function[42], while the relevant regulatory technical standard makes a distinction between critical functions[43] and critical operations[44] in relation to the recovery time set for CSDs' critical operations. Further clarification and reflection by the Union legislative bodies are warranted on the interplay between the proposed regulation and the regulatory technical standards supplementing the CSD Regulation in order to avert the risk of conflicting requirements. Finally, it should be clarified that exemptions granted to CSDs operated by certain public entities under the CSD Regulation[45] are extended under the proposed regulation.

2.3 *ESCB competences in the area of securities clearing*

2.3.1 ESCB central banks are entrusted with oversight competences in relation to central counterparties (CCPs). In this respect, the Eurosystem national central banks often cooperate with the relevant national competent authorities in the oversight and supervisory functions of CCPs and participate in the respective CCP's college established under Regulation (EU) No 648/2012 of the European Parliament and of the Council[46] (hereinafter 'EMIR'). The relevant members of the Eurosystem[47] participate in EMIR colleges in their oversight capacity and represent the Eurosystem as a central bank of issue for CCPs where the euro is one of the most relevant currencies for the financial

39 See Article 11(5) of the proposed regulation.

40 See Article 78(3) of Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (OJ L 65 10.3.2017, p. 48).

41 See Article 11(6) of the proposed regulation.

42 See Article 3(17) of the proposed regulation.

43 See Article 76(2)(d) and (e) of Commission Delegated Regulation (EU) 2017/392.

44 See Article 78(2) and (3) of Commission Delegated Regulation (EU) 2017/392.

45 See Article 1(4) of Regulation (EU) No 909/2014.

46 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

47 See Article 18(2)(g) and (h) of EMIR.

instruments cleared (and for offshore CCPs that clear a significant proportion of financial instruments in euro). The ECB is the central bank of issue for non-euro area CCPs.

2.3.2 Under the proposed regulation[48] ESCB central banks are not involved in the development of technical standards as regards the specification of ICT risks. Moreover, the proposed regulation[49] lacks any reference to the recovery time objective and the recovery point objective requirements under EMIR[50]. The proposed regulatory set-up should not provide for less restrictive requirements regarding ICT risks than those that currently exist. Hence, it is critical to set clear recovery time and point objectives in order to have a sound business continuity management framework. Maintaining specific recovery time and point objectives is also part of the CPMI-IOSCO Principles for Financial Market Infrastructures[51]. The current provision under EMIR should be retained, and the proposed regulation should be adapted accordingly. The ESCB central banks should be involved in the preparation of any secondary level legislation, as well as further clarification and reflection by the Union legislative bodies on the interplay between the proposed regulation and the regulatory technical standards supplementing, so as to avert the risk of conflicting or overlapping requirements.

3. Specific observations on prudential supervisory aspects

3.1 Council Regulation (EU) No 1024/2013[52] (hereinafter the 'SSM Regulation') confers specific tasks on the ECB concerning the prudential supervision of credit institutions within the euro area and makes the ECB responsible for the effective and consistent functioning of the Single Supervisory Mechanism (SSM), within which specific supervisory responsibilities are distributed between the ECB and the participating NCAs. In particular, the ECB has the task of authorising and withdrawing the authorisation of all credit institutions. The ECB also has the task, among others, to ensure compliance with the relevant Union laws imposing prudential requirements on credit institutions, including the requirement to have in place robust governance arrangements, such as sound risk management processes and internal control mechanisms[53]. To this end, the ECB is given all supervisory powers to intervene in the activity of credit institutions that are necessary for the exercise of its functions. The ECB and the relevant NCAs are thus the competent authorities exercising specified prudential supervisory powers under Regulation 2013/575/EU of the European Parliament and of the Council[54] (hereinafter the 'Capital Requirements Regulation') and Directive 2013/36/EU of the European Parliament and of the Council[55] (hereinafter the 'Capital Requirements Directive).

---

48 See Article 53(2)(b) and (3) of the proposed regulation and Article 34(3) of EMIR.

49 See Article 53(2)(a) of the proposed regulation.

50 See Article 34 of EMIR.

51 See CPMI-IOSCO Principles for Financial Market Infrastructures available on the website of the Bank for International Settlements: www.bis.org.

52 Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

53 See Articles 4(1)(e) and 6(4) of Regulation (EU) No 1024/2013.

54 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

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

3.2 The proposed regulation states that the single rulebook and system of supervision should be further developed to cover digital operational resilience and ICT security, by enlarging the mandates of financial supervisors tasked with monitoring and protecting financial stability and market integrity[56]. The aim is to foster a comprehensive ICT or operational risk framework through the harmonisation of key digital operational resilience requirements for all financial entities[57]. In particular, the proposed regulation aims at consolidating and upgrading ICT risk requirements that are, to date, separately addressed in different pieces of legislation[58].

3.3 The requirements related to ICT risk for the financial sector are currently spread over a number of acts of Union law, including the Capital Requirements Directive, and soft law instruments (such as EBA guidelines), and are diverse and occasionally incomplete. In some cases, ICT risk has only been implicitly addressed as part of operational risk, whereas in others it has not been addressed at all. This should be remedied by aligning the proposed regulation and those acts. To that end, the proposed amending directive puts forward a set of amendments that appear necessary to bring legal clarity and consistency in relation to the application of the various digital operational resilience requirements. However, the amendments to the Capital Requirements Directive currently suggested by the proposed amending directive[59] only refer to the provisions on contingency and business continuity plans[60], given that, purportedly, they implicitly serve as a basis for addressing ICT risk management.

3.4 Furthermore, the proposed regulation[61] provides that financial entities, including credit institutions, shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. The proposed regulation[62] provides for the application at the individual and consolidated level of the requirements set out in it, but without sufficient coordination with the sector specific legislation referred to. Last, under the proposed regulation[63], it is provided that without prejudice to the provisions on the oversight framework for critical ICT third-party service providers referred to in the proposed regulation[64], compliance with the obligations set out therein shall be ensured, for credit institutions, by the competent authority designated in accordance with Article 4 of Capital Requirements Directive, without prejudice to the specific tasks conferred on the ECB by the SSM Regulation.

3.5 In view of the foregoing, the ECB understands that, in relation to credit institutions, and save for the provisions of the proposed regulation relating to the oversight framework for critical ICT third-party service providers[65], the proposed regulation intends to set forth a prudential internal governance framework for the management of ICT risk that will be integrated into the general internal governance framework under the Capital Requirements Directive. Moreover, given the prudential nature of the

56 See Recital (8) of the proposed regulation.
57 See Recital (11) of the proposed regulation.
58 See Recital (12) of the proposed regulation.
59 See Recitals (4) and (5) of the proposed amending directive.
60 See Article 85 of the Capital Requirements Directive.
61 See Article 4(1) of the proposed regulation.
62 See Article 25(3)(4) of the proposed regulation.
63 See Article 41 of the proposed regulation.
64 See Section II of Chapter V of the proposed regulation.
65 See Section II of Chapter V of the proposed regulation.

proposed framework, the competent authorities responsible for supervision of the compliance with the obligations set out under the proposed framework, including the ECB, will be the authorities responsible for banking supervision in accordance with the SSM Regulation.

3.6 The Union legislative bodies may thus wish to take into consideration the following suggestions to increase clarity and coordination between the proposed regulation and the Capital Requirements Directive. First, the requirements under the proposed regulation may expressly be qualified as prudential, as has been done, inter alia, in the CSD Regulation[66]. Second, the recitals of the proposed amending directive[67] could broaden their wording given that the requirements under the proposed regulation go beyond the sole phase of contingency and business continuity plans. ICT risk governance measures, overall, fall under the more general scope of robust governance arrangements under Article 74 of the Capital Requirements Directive[68]. Third, the proposed regulation[69] should be amended in order to recall in the recitals the ECB's competence for the prudential supervision of credit institutions under the Treaty and the SSM Regulation. Fourth, the reference to the application at the individual and consolidated level of the requirements therein provided[70] should be revised since sub-consolidated and consolidated levels are not defined in the proposed regulation, and certain types of intermediaries are not subject to consolidated supervision under the relevant legislation (e.g. payment institutions). Moreover, the level of application of the requirements under the proposed regulation should spring solely from the legislation applicable to each type of financial entity. In the case of credit institutions, a clear connection between the Capital Requirements Directive and the proposed regulation is provided for, and so the requirements under the proposed regulation would automatically apply at individual, sub-consolidated or consolidated level[71], as the case may be. Finally, the Union legislative bodies could consider providing a transitional regime to manage the period between the entry into force of the proposed regulation and the entry into force of the regulatory technical standards envisaged in the proposed regulation, given that some intermediaries, including credit institutions, are already subject to rules on ICT risks that are applicable to specific sectors and are more detailed than the general provisions of the proposed regulation.

3.7 The ECB has been entrusted under the SSM Regulation with the task of ensuring compliance by credit institutions with Union law requirements requiring credit institutions to have in place robust risk management processes and internal control mechanisms[72]. This means that the ECB must ensure that credit institutions implement policies and processes to evaluate and manage their exposure to operational risk, including model risk, and to cover low-frequency, high-severity events. Credit

66 See title of Chapter II, Section 4, "Prudential requirements" of the CSD Regulation.
67 See Recital (4) of the proposed amending directive.
68 Article 85 of Directive 2013/36/EU is a mere specification. In this regard, please see also pages 4, 11 and 37 of the European Banking Authority Guidelines on ICT and security risk management of 29 November 2019 (hereinafter the 'EBA Guidelines'), where the general legal basis is expressly found in Article 74 of Directive 2013/36/EU.
69 See Article 41(1) of the proposed regulation.
70 See Article 25(3) and (4) of the proposed regulation.
71 See also Article 109 of the Capital Requirements Directive.
72 See Article 4(1)(e) of the SSM Regulation.

institutions are required to articulate what constitutes operational risk for the purposes of these policies and procedures[73].

3.8 In July 2017 the Governing Council of the European Central Bank (ECB) adopted the SSM Cyber Incident Reporting Framework (hereinafter referred to as the 'Framework'), on the basis of a draft proposal of the Supervisory Board in accordance with Articles 26(8) and Article 6(2) of the SSM Regulation and Article 21(1) of Regulation (EU) No 468/2014 of the European Central Bank (ECB/2014/17)[74]. The Framework consists of a binding request (individual decisions addressed to credit institutions) for information and/or reporting on the basis of Article 10 of the SSM Regulation[75]. Some countries already have an incident reporting process in place, requiring credit institutions to report all significant cyber incidents to their NCAs. In those countries, significant credit institutions will still report incidents to the NCAs, which will then forward them without undue delay to the ECB on behalf of the supervised entities. Therefore, the decisions referred to above are also addressed to these national competent authorities to forward that information to the ECB based on the Framework. The ECB supports the Union legislative bodies' effort to promote harmonisation and streamlining, inter alia, regarding the set of rules and obligations applicable to credit institutions on incident reporting. In view of this, the ECB stands ready to amend (and potentially repeal) the Framework, where necessary, in the light of the eventual adoption of the proposed regulation.

4. Specific observations on ICT risk management, incident reporting, operational resilience testing and ICT third-party risk

4.1 *ICT risk management*

4.1.1 The ECB welcomes the introduction by the proposed regulation of a robust and comprehensive ICT risk management framework that encompasses the CPMI-IOSCO Guidance on cyber resilience and is closely aligned to best practices, including the Eurosystem Cyber Resilience Oversight Expectations for FMIs.

4.1.2 The ECB supports the notion that financial entities should have to perform risk assessments upon each 'major change' in the network and information system infrastructure [76]. Having said that, the proposed regulation contains no definition of 'major change', creating unwelcome scope for diverging interpretations by financial entities that could ultimately hamper the proposed regulation's harmonisation aims. For the sake of legal certainty, the Union legislative bodies might wish to consider the introduction of a definition of 'major change' in the proposed regulation.

---

73 See Article 85 of the Capital Requirements Directive.

74 Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ L 141, 14.5.2014, p. 1).

75 Specifically, a cyber incident (an identified possible breach of information security, whether malicious or accidental) must be reported to the ECB if at least one of the following conditions is met: (1) there is a potential financial impact of €5 million or 0.1% of CET1; (2) the incident is publicly reported or causes reputational damage; (3) the incident was escalated to the CIO outside of the regular reporting; (4) the bank notified the incident to the CERT/CSIRT, a security agency or the police; (5) disaster recovery or business continuity procedures have been triggered or a cyber insurance claim has been filed; (6) there has been a breach of legal or regulatory requirements; or (7) the bank uses internal criteria and expert judgement (including a potential systemic impact) and decides to inform the ECB.

76 See Article 7(3) of the proposed regulation.

4.1.3 The ECB generally supports the idea that financial entities other than microenterprises shall report relevant costs and losses caused by ICT disruptions and ICT related incidents to competent authorities[77]. However, to ensure the overall effectiveness of the system, and to avoid the possibility of overwhelming competent authorities and financial entities with an excessive number of reports, the introduction of relevant thresholds, possibly of a quantitative nature, could be usefully explored by the Union legislative bodies.

4.1.4 The ECB acknowledges the possibility of financial entities delegating to intra-group or external undertakings the tasks of verifying compliance with ICT risk management requirements, upon approval by the competent authorities[78]. At the same time, it is important that the Union legislative bodies clarify how the approval by the competent authorities would be granted in cases where a financial entity is subject to multiple competent authorities. This could occur where a financial entity is a credit institution, a crypto-assets service provider and/or a payment service provider. Finally, in relation to the identification and classification to be performed by financial entities under the proposed regulation[79], the ECB would consider prudent, for the purposes of the classification of assets, that the proposed regulation also require financial entities to take into account the criticality of such assets (i.e. whether they support critical functions).

4.2 *Incident reporting*

4.2.1 The ECB welcomes the efforts outlined in the proposed regulation to harmonise the ICT incident reporting landscape within the Union and work towards a centralised reporting of major ICT-related incidents[80]. The introduction of a harmonised framework for the reporting of major ICT-related incidents[81] to the relevant competent authorities would in principle streamline and harmonise the reporting burden of financial entities, including credit institutions. Competent authorities would benefit from the broader scope of incidents covered, going beyond cyber-related incidents currently covered by existing frameworks[82]. The future adoption of the proposed regulation would require reviewing and potentially repealing existing frameworks, including the SSM Cyber Incident Reporting Framework. Having said that, in order to achieve a true streamlining and full alignment across all frameworks, it is critical to ensure that the scope of the incident reporting provisions under the proposed regulation, including all the relevant definitions, thresholds and reporting parameters, be fully aligned with relevant frameworks. In particular, it is of the utmost importance to ensure alignment between on the one hand the proposed regulation, and, on the other hand, Directive (EU) 2015/2366 of the European Parliament and of the Council[83] (hereinafter the 'PSD2') and the EBA Guidelines on major incident reporting (hereinafter the 'EBA Guidelines'). The proposed amending directive[84] contains amendments to the PSD2 in relation to the delineation of the incident reporting between the

77 See Article 10(9) of the proposed regulation.
78 See Article 5(10) of the proposed regulation.
79 See Article 7 of the proposed regulation.
80 See Article 19 of the proposed regulation.
81 See Articles 3(7), 17 and 18 of the proposed regulation.
82 See for example the Framework.
83 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).
84 See Article 7(9) of the proposed amending directive.

proposed regulation and the PSD2, which would affect mainly payment service providers, who could also be authorised as credit institutions, as well as the competent authorities. There is a lack of clarity as regards the incident notification process, and there is a potential overlap between some of the incidents that need to be reported under both the proposed regulation and the EBA Guidelines.

4.2.2 The processes for notifying major incidents under, respectively, the proposed regulation[85], the PSD2 and the corresponding EBA Guidelines would require payment service providers to submit an incident report to their respective competent authority once the incident has been classified. As a matter of fact, initial reports do not capture the essence, cause or functional area affected by the incident and payment service providers may only be in a position to make such distinctions at a later stage, when more detailed information about the incident becomes available. As a result, initial incidents reports could be submitted both under the proposed regulation and the EBA Guidelines, or payment service providers may decide upon a single reporting framework and correct their submissions at a later date. The same uncertainty (as regards, for instance, the root cause of any incident) may also be reflected in intermediate and final reports. This would once again raise the potential for parallel submission of reports to the competent authorities under the proposed regulation and the PSD2.

4.2.3 Some incidents that may be categorised as ICT-related incidents may also have an impact on other areas and, as a result, would need to be notified under the EBA Guidelines. This may be the case where an incident has an impact from an ICT perspective but, at the same time, has also affected the provision of payment services directly and/or other non-ICT functional areas or channels. In addition, there could be instances where it is not possible to distinguish between operational and ICT-related incidents. Furthermore, in the case where the same financial entity is a significant credit institution and a payment service provider, under the proposed regulation the same entity would have to report the ICT-related incident twice, being subject to two competent authorities. In view of the foregoing, the proposed regulation should articulate more clearly how the interplay between the PSD2 and the EBA Guidelines is meant to work in practice. More significantly, it would be important, for the sake of harmonisation and streamlining of reporting obligations, that the Union legislative bodies reflect on residual issues of double reporting, and that it clarify whether the proposed regulation on the one hand, and the PSD2 and EBA Guidelines on the other hand, would co-exist, or whether there should be a single set of incident reporting requirements.

4.2.4. The proposed regulation introduces a requirement for the competent authorities[86], upon receipt of a report, to acknowledge receipt of notification and as quickly as possible to provide all necessary feedback or guidance to the financial entity, in particular to discuss remedies at the level of the entity or ways to minimise the adverse impact across sectors. This would mean that the competent authorities should actively contribute to managing and remediating incidents while at the same time also assessing the response of a supervised entity to critical incidents. The ECB emphasises that the responsibility for and ownership of the remediation and the consequences of an incident should remain solely and clearly with the financial entity concerned. The ECB would therefore propose to limit the feedback and guidance to high-level prudential feedback and guidance only. If feedback

85 See Article 17(3) of the proposed regulation.
86 See Article 20 of the proposed regulation.

were wider, it would require specialised professionals with very considerable technical knowledge not typically available in the talent pool available to prudential authorities.

4.3 *Digital operational resilience testing*

4.3.1 The ECB welcomes the requirements set out under the proposed regulation[87] on digital operational resilience testing across financial entities and the need for each institution to have its own testing programme. The proposed regulation[88] describes different types of tests as indicatory to financial entities. The types of tests are not very clear and some tests, such as compatibility tests, questionnaires, or scenario-based tests, are open to interpretation by ESAs, competent authorities or financial entities. In addition, there is also no guidance as to the frequency of each test. A possible approach could be that the proposed regulation would set out generic testing requirements, with a more precise description of the types of tests being set out in regulatory and implementing technical standards.

4.3.2 Threat-led penetration testing (TLPT) is a powerful tool to test security defences and preparedness. The ECB therefore encourages TLPT by financial entities. With this tool not only technical measures are tested, but also staff and processes. The results of these tests can significantly increase the security awareness of the senior management within the entities being tested. The European Framework for Threat Intelligence Based Ethical Red-teaming (TIBER-EU)[89] and other TLPT tools already available, outside the Union, are primary instruments for entities themselves to assess, test, practise and improve their cyber resilience posture and defences.

4.3.3 In most Member States where TIBER-EU has been implemented, overseers and supervisors do not play an active role in the implementation of a localised TIBER-XX program and the TIBER Cyber Team (TCT) is situated in almost all cases independently of these functions. For this reason, advanced testing under the proposed regulation[90], by means of TLPT, should be implemented as a tool to strengthen the financial ecosystem and enhance financial stability rather than a purely supervisory tool. In addition, there is no need for the development of a new advanced cyber resilience testing framework as Member States have already widely adopted TIBER-EU, the only such framework in the EU at present.

4.3.4 Requirements for testers should not be contained in the main body of the proposed regulation, as the TLPT-related sector is still developing and innovation may be hindered by mandating specific requirements. Having said that, the ECB is of the view that in order to ensure a high degree of independence when conducting tests, financial entities should not employ or contract testers that are employed or contracted by financial entities in their own group or that are otherwise owned and/or controlled by the financial entities to be tested.

4.3.5 In order reduce the risk of fragmentation and ensure harmonisation, the proposed regulation should mandate one TLPT framework that applies to the financial sector across the Union. Fragmentation may lead to increases in terms of costs, and of technical, operational and financial resource requirements, for both competent authorities and financial institutions. These increased costs and

87 See Articles 21 and 22 of the proposed regulation.
88 See Article 22(1) of the proposed regulation.
89 Available on the ECB's website at www.ecb.europa.eu.
90 Articles 23 and 24 of the proposed regulation.

requirements may ultimately have a negative impact on the mutual recognition of tests. This lack of harmonisation and the resulting issues with mutual recognition are especially critical for financial entities, which may hold multiple licences and/or operate in multiple jurisdictions across the Union. The regulatory and implementing technical standards, which are to be drafted for TLPT under the proposed regulation, should be in accordance with TIBER-EU. Furthermore, the ECB welcomes the opportunity to be involved in the preparation of these regulatory and implementing technical standards in cooperation with the ESAs.

4.3.6 The active involvement of competent authorities in the tests could result in a potential conflict of interest with the other function they perform, i.e. assessing the financial entity's testing framework. Against this background, the ECB proposes to remove from the proposed regulation any obligation for competent authorities regarding the validation of documents and the issuance of an attestation for a TLPT test.

4.4 *ICT third-party risk*

4.4.1 The ECB welcomes the introduction of a comprehensive set of key principles and a robust oversight framework to identify and manage ICT risks stemming from ICT third-party service providers, regardless of whether these belong to the same group of financial entities. Having said that, in order to achieve an effective ICT risk identification and management, it is important to correctly identify and classify, inter alia, critical ICT third-party service providers. In this regard, while the introduction of delegated acts[91] that will supplement the criteria to be used for classification purposes[92] is welcomed, the ECB should be consulted prior to the adoption of such delegated acts.

4.4.2 As regards the structure of the oversight framework[93], further clarification is needed with respect to the role to be undertaken by the Joint Committee. At the same time, the ECB welcomes its inclusion in the Oversight Forum as an observer, as this role will provide the ECB with the same access to documentation and information as voting members[94]. The ECB would like to draw the Union legislative bodies' attention to the fact that the ECB, in its role as an observer, would contribute to the work of the Oversight Forum both in its capacity as a central bank of issue, with responsibility for the oversight of market infrastructures, and as prudential supervisor of credit institutions. In addition, the ECB notes that, besides being an observer in the Oversight Forum, the ECB would also, as competent authority, be part of the joint examination team. In this respect, further reflection by the Union legislative bodies could be given to the composition of the joint examination teams[95] so as to ensure an appropriately weighty involvement of the relevant competent authorities. By the same token, the ECB believes that the maximum number of participants in the joint examination teams should be increased, taking into account the criticality, the complexity and the scope of the ICT third-party services.

4.4.3 The ECB notes that under the proposed regulation the lead overseer may prevent critical ICT third-party service providers from entering into further subcontracting arrangements where (i) the

91 See Article 28(3) of the proposed regulation.
92 See Article 28(2) of the proposed regulation.
93 See Article 29 of the proposed regulation.
94 See Article 29(3) of the proposed regulation.
95 See Article 35 of the proposed regulation.

envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country and (ii) the subcontracting concerns a critical or important function of the financial entity. The ECB wishes to highlight that these powers can only be exercised by the lead overseer in the context of subcontracting arrangements where a critical ICT third-party service provider subcontracts a critical or important function to a separate legal entity established in a third country. The ECB understands that the lead overseer could not exercise comparable powers to prevent a critical ICT third-party service provider from outsourcing critical or important functions of the financial entity to facilities of that service provider that are located in a third country. It could be the case, for example, that, from an operational standpoint, critical data and/or information may be stored or processed by facilities located outside the European Economic Area (EEA). In such a case, the powers of the lead overseer may not adequately empower the competent authorities to access all information, premises, infrastructures and personnel relevant for the performance of all critical or important functions of the financial entity. In order to ensure that the ability of competent authorities to perform their tasks unhindered, the ECB suggests that the lead overseer should be granted the power to also restrict the use by critical ICT third-party service providers of facilities located outside the EEA. This power could be exercised in those specific cases where administrative arrangements with the relevant third country authorities, as provided under the proposed regulation are not in place[96], or the representatives of the critical ICT third-party service providers fail to provide sufficient reassurances under the framework of the relevant third country as to the access to the information, premises, infrastructure and personnel which is needed to conduct oversight or supervisory tasks.

4.4.4 Finally, requiring the competent authorities to follow up on the recommendations of the lead overseer[97] could risk proving ineffective, as competent authorities may not have a holistic view of the risks generated by each critical ICT third-party service provider. In addition, the competent authorities may be required to take actions against their supervised financial entities where the recommendations are not addressed by the critical third-party service providers. Under the proposed regulation[98], the competent authorities may require their supervised financial entities to temporarily suspend the critical third-party service or to terminate outstanding contracts with critical third-party service providers. It is difficult to translate the envisaged follow-up process into concrete actions. Specifically, it is not clear whether a supervised financial entity will be in a position to suspend or terminate a contract with a critical third-party service provider. This is because the critical ICT third-party service provider could be a significant provider for that financial entity, or because of the costs and damages, contractual or otherwise, that the financial entity may suffer as a consequence of such a suspension or termination. Moreover, this approach is not supportive of oversight convergence, since competent authorities may interpret the same recommendation in divergent manner. This could ultimately hamper the envisaged harmonisation and consistent approach in the monitoring of critical ICT third-party risk at the Union level. In view of the foregoing, the Union legislative bodies may wish to consider granting the legal overseers specific enforcement powers vis-à-vis critical ICT third party

96 See Article 39(1) of the proposed regulation.
97 See Article 29(4) and Article 37 of the proposed regulation.
98 See Article 37(3) of the proposed regulation.

service providers, taking into account the limits imposed by the *Meroni* doctrine, as partially mitigated by the Court of Justice in its judgement in the ESMA case[99].

Where the ECB recommends that the proposed regulation be amended, specific drafting proposals are set out in a separate technical working document accompanied by an explanatory text to this effect. The technical working document is available in English on EUR-Lex.

Done at Frankfurt am Main, 4 June 2021.

The President of the ECB

Christine LAGARDE

99 See Judgment of the Court (Grand Chamber), 22 January 2014 United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union Regulation (EU) No 236/2012 — Case C-270/12.

EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

Technical working document

produced in connection with ECB Opinion CON/2021/20[1]

Drafting proposals in relation to a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and a proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EC, EU/2011/61, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341

Drafting proposals in relation to a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA)

Text proposed by the European Commission	Amendments proposed by the ECB[2]
Amendment 1 Recitals (new recital 7a)	
	'(7a) Pursuant to the fourth indent of Article 127(2) TFEU, one of the basic tasks to be carried out through the European System of Central Banks (ESCB) is to promote the smooth operation of payment systems. The European Central Bank (ECB) may, pursuant to Article 22 of the Statute of the European System of Central Banks and of the European Central Bank, make regulations to ensure efficient and sound clearing and payment systems within the Union and with other countries. In this respect, the ECB has adopted regulations on requirements for systemically important payment systems. This Regulation is without prejudice to the responsibilities of the ECB and the national central banks (NCBs) in the ESCB to ensure efficient and sound clearing and

1 This technical working document is produced in English only and communicated to the consulting Union institution(s) after adoption of the opinion. It is also published on EUR-Lex alongside the opinion itself.

2 Bold in the body of the text indicates where the ECB proposes inserting new text. Strikethrough in the body of the text indicates where the ECB proposes deleting text.

Text proposed by the European Commission	Amendments proposed by the ECB[2]
	payment systems within the Union and with other countries. Consequently, the access to information by the ECB and the NCBs is crucial when fulfilling their tasks relating to the oversight of clearing and payment systems. Moreover, payment systems, instruments, schemes and arrangements, as well as systems operated, facilities offered and services provided by ESCB central banks, and critical service providers subject to existing ESCB and Eurosystem oversight frameworks, should all be excluded from the scope of application of this Regulation. Further, and in order to prevent the possible creation of parallel sets of rules, the ESAs, and the ESCB should cooperate closely when preparing the relevant draft technical standards.'
Explanation *In view of the close links between the provisions of the proposed regulation and the oversight competences of the ECB and the ESCB under the Treaty, reference to these competences should be explicitly mentioned in the proposed regulation. See paragraph 2.1 of the ECB Opinion.*	
Amendment 2 Recital (recital 8)	
'(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than for example common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this	'(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not **yet** fully or consistently harmonised ~~yet~~, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than**,** for example**,** common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this

2

Text proposed by the European Commission	Amendments proposed by the ECB[2]
component, by enlarging the mandates of financial supervisors tasked to monitor and protect financial stability and market integrity.'	component, by enlarging the ~~mandates~~ **powers** of financial supervisors **responsible for the prudential supervision of the financial sector and** ~~to~~ **for** monitor**ing** and protect**ing** financial stability and market integrity.'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, reference to these prudential supervision competences should be explicitly mentioned in the proposed regulation. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.*	
Amendment 3 Recitals (recital 12)	
'(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements addressed so far separately in the different Regulations and Directives. While those [...]'	(12) This Regulation aims first at consolidating and upgrading the ~~ICT risk~~ **prudential** requirements **on ICT risks** addressed so far separately in the different Regulations and Directives. While those [...]'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, an explicit reference to the prudential nature of the requirements in the proposed regulation should be made. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.*	
Amendment 4 Recitals (recital 67)	
'(67) Competent authorities should possess all necessary supervisory, investigative and sanctioning powers to ensure the application of this Regulation. Administrative penalties should, in principle, be published. Since financial entities and ICT third-party service providers can be	'(67) **Supervision of the compliance of financial entities with the prudential requirements of this Regulation should be entrusted to the competent authorities referred to in the relevant sector specific legislation, including the ECB in accordance with Regulation (EU) No**

Text proposed by the European Commission	Amendments proposed by the ECB[2]
established in different Member States and supervised by different sectoral competent authorities, close cooperation between the relevant competent authorities, including ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/201339, and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities.'	**1024/2013.** Competent authorities should possess all necessary supervisory, investigative and sanctioning powers to ensure the application of this Regulation. Administrative penalties should, in principle, be published. Since financial entities and ICT third-party service providers can be established in different Member States and supervised by different sectoral competent authorities, close cooperation between the relevant competent authorities~~, including ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/201339,~~ and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities.'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, it would be helpful to explicitly reference the competences of the ECB for the direct supervision of significant credit institutions, in order to ensure regulatory clarity on the attribution of competences. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.*	
Amendment 5 Article 1(1) and new paragraph (3)	
'1. This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience, as follows: (a) requirements applicable to financial entities in relation to: […]	'1. This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience, as follows: (a) **prudential** requirements applicable to financial entities in relation to: […]

Text proposed by the European Commission	Amendments proposed by the ECB[2]
(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities; [...]'	(b) **prudential** requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities; [...] **3. The prudential requirements laid down under points (a) and (b) of paragraph 1 shall apply on an individual, consolidated or sub-consolidated level, in accordance with the level of application of general governance requirements provided in the relevant sector specific legislation.**'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, explicit reference to the prudential nature of the requirements of this regulation should be made. To fully ensure regulatory consistency and clarity across the sectoral frameworks, it is also useful to generally clarify that the prudential requirements under the proposed regulation apply on an individual, consolidated or sub-consolidated level, in accordance with the level of application of general governance requirements provided in the relevant sector specific legislation. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.*	
Amendment 6 Article 7(1)	
'1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.'	'1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation. **Financial entities shall classify the assets**

Text proposed by the European Commission	Amendments proposed by the ECB[2]
	referred to in this paragraph by taking the criticality of such assets into account.'
Explanation *In relation to the identification and classification to be performed by financial entities under the proposed regulation, the ECB suggests, for the purposes of the classification of assets, that the proposed regulation also requires financial entities to take the criticality of such assets into account. See paragraph 4.1.4 of the ECB Opinion.*	
Amendment 7 Article 23	
'1. Financial entities identified in accordance with paragraph 4 shall carry out at least every 3 years advanced testing by means of threat led penetration testing.	'1. Financial entities identified in accordance with paragraph 4 shall carry out at least every 3 years advanced testing by means of threat led penetration testing.
2. Threat led penetration testing shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities.	2. Threat led penetration testing shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting ~~such~~ **these services and** functions. The precise scope of ~~threat led penetration~~ **the** test~~ing,~~ **shall be** based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the ~~competent~~ **appropriate** authorit~~ies~~**y.**
For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or contracted to ICT third-party service providers.	For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or contracted to ICT third-party service providers.
Where ICT third-party service providers are included in the remit of the threat led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers.	Where ICT third-party service providers are included in the remit of the threat led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers.

Text proposed by the European Commission	Amendments proposed by the ECB[2]
Financial entities shall apply effective risk management controls to reduce the risks of any potential impact to data, damage to assets and disruption to critical services or operations at the financial entity itself, its counterparties or to the financial sector.	Financial entities shall apply effective risk management controls to reduce the risks of any potential impact to data, damage to assets and disruption to critical services or operations at the financial entity itself, its counterparties or to the financial sector.
At the end of the test, after reports and remediation plans have been agreed, the financial entity and the external testers shall provide to the competent authority the documentation confirming that the threat led penetration testing has been conducted in accordance with the requirements. Competent authorities shall validate the documentation and issue an attestation.	~~At the end of the~~ **Upon completion of the threat led penetration** testing, after reports and remediation plans have been agreed, the financial entity ~~and the external testers~~ shall provide to the competent authority ~~the~~ documentation confirming that the ~~threat led penetration~~ testing has been conducted in accordance with the requirements. ~~Competent authorities shall validate the documentation and issue an attestation.~~
3. Financial entities shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.	3. Financial entities shall contract **suitable and reputable external** testers ~~in accordance with Article 24~~ for the purposes of undertaking threat led penetration testing. .
Competent authorities shall identify financial entities to perform threat led penetration testing in a manner that is proportionate to the size, scale, activity and overall risk profile of the financial entity, based on the assessment of the following:	Competent authorities shall identify **which** financial entities ~~to perform threat led penetration testing~~ **should undergo threat led penetration testing** ~~in a manner that is proportionate to the~~ **by taking into account the financial entity's** size, scale, activity and overall risk profile of the financial entity, based on the assessment of the following:
(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;	(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;
(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;	(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;
(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved.	(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features ~~which are~~ involved**;**
	(d) proportionality considerations.

Text proposed by the European Commission	Amendments proposed by the ECB[2]
4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further: (a) the criteria used for the purpose of the application of paragraph 6 of this Article; (b) the requirements in relation to: (i) the scope of threat led penetration testing referred to in paragraph 2 of this Article; (ii) the testing methodology and approach to be followed for each specific phase of the testing process; (iii) the results, closure and remediation stages of the testing; (c) the type of supervisory cooperation needed for the implementation of threat led penetration testing in the context of financial entities which operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.. The ESAs shall submit those draft regulatory technical standards to the Commission by [*OJ: insert date 2 months before the date of entry into force*]. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.'	4. EBA, ESMA and EIOPA shall, after consulting the ECB**, and in accordance with TIBER-EU,** ~~and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests,~~ develop draft regulatory technical standards to specify further **the**: (a) ~~the~~ criteria used to identify financial entities for the purposes of paragraph ~~6~~**1** of this Article; (b) ~~the~~ requirements in relation to **the**: (i) ~~the~~ scope of threat led penetration testing referred to in paragraph 2 of this Article; ~~(ii) the testing methodology and approach to be followed for each specific phase of the testing process;~~ (iii) ~~the~~ results, closure and remediation stages of the testing; **and** (c) ~~the~~ type of supervisory cooperation needed for the implementation of threat led penetration testing in the context of financial entities **that** ~~which~~ operate in more than one Member State, **so as** to allow an appropriate level of supervisory involvement and ~~a~~ flexible implementation t**hat** ~~o~~ cater**s** ~~for~~ **to the** specificities of financial sub-sectors **and** ~~or~~ local financial markets. The ESAs**, after consultation with the ECB,** shall submit those draft regulatory technical standards**, if any,** to the Commission by [*OJ: insert date 2 months before the date of entry into force*]. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.'
Explanation	

8

Text proposed by the European Commission	Amendments proposed by the ECB[2]
The ECB proposes changes to clarify Article 23 of the proposed regulation on TLPT and to include a reference for the testers in light of the proposed deletion referred to in Amendment 8 below. Furthermore, in order to reduce the risk of fragmentation and ensure harmonisation, the proposed regulation should mandate one TLPT framework that applies to the financial sector across the Union. Fragmentation may lead to increases in terms of costs and of technical, operational and financial resource requirements for both competent authorities and financial institutions. These increased costs and requirements may ultimately have a negative impact on the mutual recognition of tests. For these reasons, the regulatory and implementing technical standards which are to be drafted for TLPT under the proposed regulation should be in accordance with TIBER-EU. Furthermore, the ECB welcomes the opportunity to be involved in the preparation of these regulatory and implementing technical standards in cooperation with the ESAs. See paragraphs 4.3.2 to 4.3.6 of the ECB Opinion.	
Amendment 8 Article 24	
'1. Financial entities shall only use testers for the deployment of threat led penetration testing, which: (a) are of the highest suitability and reputability; (b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing; (c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks; (d) in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity; (e) in case of external testers, are dully and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.	~~'1. Financial entities shall only use testers for the deployment of threat led penetration testing, which:~~ ~~(a) are of the highest suitability and reputability;~~ ~~(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing;~~ ~~(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;~~ ~~(d) in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;~~ ~~(e) in case of external testers, are dully and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.~~

Text proposed by the European Commission	Amendments proposed by the ECB[2]
2. Financial entities shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.'	~~2. Financial entities shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.~~'
Explanation *Where advanced testing remains mandatory, the ECB proposes to delete Article 24 of the proposed regulation. This is because, based on the ECB's experience with TIBER-EU, the TLPT-related sector is still developing and innovation may be hindered by mandating specific requirements in the proposed regulation. See paragraph 4.3.4 of the ECB Opinion.*	
Amendment 9 Article 25(3) and (4)	
'3. As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in point (g) of Article 5(9). That strategy shall include a policy on the use of ICT services provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions. 4. As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. […]. '	'3. As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in point (g) of Article 5(9). That strategy shall include a policy on the use of ICT services provided by ICT third-party service providers ~~and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis~~. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions. 4. As part of their ICT risk management framework, financial entities shall maintain and update ~~at entity level and, at sub-consolidated and consolidated levels,~~ a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. […]. '

Text proposed by the European Commission	Amendments proposed by the ECB[2]
Explanation *For prudential supervisory reasons, the reference to the application at the individual and consolidated level should be revised since sub-consolidated and consolidated levels are not defined in the proposed regulation, and certain types of intermediaries are not subject to consolidated supervision under the applicable legislation (e.g. payment institutions). Moreover, the level of application of the requirements under the proposed regulation should only depend on the legislation applicable to each type of intermediary. For credit institutions, it is suggested to amend the Capital Requirements Directive to create a clear renvoi from the Capital Requirements Directive to the proposed regulation (see Amendments 1 and 2 to the proposal for a directive amending, inter alia, Directive EU/2013/36 below). If such a renvoi is introduced into the Capital Requirements Directive, the requirements under the proposed regulation would automatically apply at either the individual, sub-consolidated or consolidated level in accordance with Article 109 of the Capital Requirements Directive. See paragraph 3.6 of the ECB Opinion.*	
Amendment 10 Article 28(3)	
'3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement the criteria referred to in paragraph 2.'	'3. The Commission is empowered to adopt**, after consulting with the ECB,** delegated acts in accordance with Article 50 to supplement the criteria referred to in paragraph 2.'
Explanation *In order to achieve an effective ICT risk identification and management, the ECB considers it important to correctly identify and classify, inter alia, critical ICT third-party service providers. In this regard, while the ECB welcomes the introduction of delegated acts that will supplement the criteria to be used for classification purposes, it is suggested that the ECB should be consulted prior to the adoption of these delegated acts. See paragraph 4.4.1 of the ECB Opinion.*	
Amendment 11 New Article 31(1)(d)(v)	
	'**(v) refraining from using facilities located outside the European Economic Area for the purpose of storing or processing critical data and/or information that may be relevant for the performance of all critical or important functions of the financial entity and for the performance of tasks by the competent**

Text proposed by the European Commission	Amendments proposed by the ECB[2]
	authorities, where administrative arrangements with the relevant third country authorities or the representatives of the critical ICT third-party service providers fail to provide sufficient reassurances under the framework of the relevant third country as to the access to the information, premises, infrastructure and personnel which is needed to conduct oversight or supervisory tasks.'
Explanation *The ECB understands that the lead overseer could not exercise comparable powers to prevent a critical ICT third-party service provider from outsourcing critical or important functions of the financial entity to facilities of that service provider that are located in a third country. It could be the case, for example, that, from an operational standpoint, critical data and/or information may be stored or processed by facilities located outside the European Economic Area (EEA). In such a case, the powers of the lead overseer may not adequately empower the competent authorities to access all information, premises, infrastructures and personnel relevant for the performance of all critical or important functions of the financial entity. To ensure the ability of competent authorities to perform their tasks unhindered, the ECB suggests that the lead overseer be granted the power to also restrict the use by critical ICT third-party service providers of facilities located outside the EEA. This power should only be exercised in those specific cases where administrative arrangements with the relevant third country authorities or the representatives of the critical ICT third-party service providers fail to provide sufficient reassurances under the framework of the relevant third country as to the access to the information, premises, infrastructure and personnel which is needed to conduct oversight or supervisory tasks. See paragraph 4.4.3 of the ECB Opinion.*	
Amendment 12 Article 44	
'1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.' 2. The powers referred to in paragraph 1 shall include at least the powers to; […]	'1. **To the extent not already provided under the relevant sector specific legislation,** ~~C~~competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation. 2. The powers referred to in paragraph 1 shall include at least the powers to:

Text proposed by the European Commission	Amendments proposed by the ECB[2]
(c) require corrective and remedial measures for breaches of the requirements of this Regulation. 3. Without prejudice to the right of Member States to impose criminal penalties according to Article 46, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation. Those penalties and measures shall be effective, proportionate and dissuasive. 4. Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation: [...] 5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach. 6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.'	[...] (c) require ~~corrective and~~ remedial measures for breaches of the requirements of this Regulation. 3. Without prejudice to the right of Member States to impose criminal penalties according to Article 46, Member States shall **ensure** ~~lay down~~ rules **are laid down** establishing appropriate administrative penalties and remedial measures for breaches of this Regulation ~~and shall ensure their effective implementation~~. Those penalties and measures shall be effective, proportionate and dissuasive. 4. ~~Member States shall confer on~~ **To the extent not already provided for in the relevant sector specific legislation,** competent authorities **shall have** the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation: [...] 5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, ~~Member States shall confer on~~ competent authorities **shall have** the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach. 6. ~~Member States shall ensure that a~~ **A**ny decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 ~~is~~ **shall be** properly reasoned**. Member States shall ensure that these decisions** ~~and is~~ **are** subject to a right of appeal.'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities for the prudential supervision of credit institutions under the*	

Text proposed by the European Commission	Amendments proposed by the ECB[2]
SSM Regulation and the Capital Requirements Directive, as well as to ensure regulatory consistency and avoid duplication and conflicting requirements, reference should be made to the relevant sector specific legislation, as long as such legislation already ensures the same level of harmonisation as the proposed regulation. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.	
Amendment 13 Article 45(1) and (2)	
'1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 44 in accordance with their national legal frameworks, as appropriate: [...] 2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate: [...]'	'1. Competent authorities shall exercise the power~~s~~ to impose administrative penalties and remedial measures ~~referred to in Article 44~~in accordance with **the relevant sector specific legislation** ~~their national legal frameworks~~, as appropriate: [...] 2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed ~~under Article 44~~, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate: [...]'
Explanation *See explanation for Amendment 12 above.*	
Amendment 14 Article 48(1)	
'1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no right of appeal after the addressee of the sanction has been notified of that decision.'	'1. **To the extent not already provided for in the relevant sector specific legislation,** ~~C~~competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no right of appeal after the addressee of the sanction has been notified of that decision.'
Explanation *See explanation for Amendment 12 above.*	

Text proposed by the European Commission	Amendments proposed by the ECB[2]
Amendment 15 Article 49 new paragraph 5	
	'5. This Article shall apply only when confidential information received, exchanged or transmitted pursuant to this Regulation is not already subject to equivalent provisions on professional secrecy under the relevant sector specific legislation.'
Explanation *Articles 53-62 of the Capital Requirements Directive contain detailed provisions governing the exchange of information and professional secrecy. These provisions are more detailed than those applicable under Article 49 of the proposed regulation. In view of the importance of this matter, it is suggested that these provisions of the Capital Requirements Directive should not be supplanted by the more limited provisions under Article 49 of the proposed regulation. It is therefore suggested to explicitly clarify that Article 49 of the proposed regulation shall apply only when confidential information received, exchanged or transmitted pursuant to the proposed regulation is not already subject to equivalent provisions on professional secrecy under the relevant sector specific legislation. See paragraphs 3.1, 3.5 and 3.6 of the ECB Opinion.*	
Amendment 16 Article 53(2) (a), (b) and (3) (amending Regulation (EU) 648/2012)	
'2. Article 34 is amended as follows:	'2. Article 34 is amended as follows:
(a) paragraph 1 is replaced by the following:	~~(a) paragraph 1 is replaced by the following:~~
'1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.	~~'1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.~~'
(b) in paragraph 3, the first subparagraph is replaced by the following: In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop	(b) in paragraph 3, the first subparagraph is replaced by the following: In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop

Text proposed by the European Commission	Amendments proposed by the ECB[2]
draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity and disaster recovery plans. (3) in Article 56, the first subparagraph of paragraph 3 is replaced by the following: 3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for registration referred to in paragraph 1.'	draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan~~, excluding ICT business continuity and disaster recovery plans.~~' (3) in Article 56, the first subparagraph of paragraph 3 is replaced by the following: 3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details~~, other than for requirements related to ICT risk management,~~ of the application for registration referred to in paragraph 1.'
Explanation *It is critical to set clear recovery time and point objectives in order to have a sound business continuity management framework. Having specific recovery time and point objectives is also in line with international standards such as the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs). It is therefore proposed to retain Article 34(1) of EMIR. Finally, the involvement of the ESCB central banks in the preparation of the secondary level legislation, as well as further clarification and reflection by the Union legislative bodies are warranted on the interplay between the proposed regulation and the regulatory technical standards supplementing EMIR in order to avert the risk of conflicting or overlapping requirements. See paragraph 2.3.2 of the ECB Opinion.*	
Amendment 17 Article 54(4) and (5) (amending Regulation (EU) 909/2014)	
'4. in paragraph 6, the first subparagraph is replaced by the following: 'A CSD shall identify, monitor and manage the risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of	'4. in paragraph 6, the first subparagraph is replaced by the following: 'A CSD shall identify, monitor and manage the risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of

Text proposed by the European Commission	Amendments proposed by the ECB[2]
any operational incidents, other than in relation to ICT risk, resulting from such risks.'; 5. in paragraph 7, the first subparagraph is replaced by the following: 'ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risks, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.' [...]'	any operational incidents ~~other than in relation to ICT risk, resulting from such risks.~~'; 5. in paragraph 7, the first subparagraph is replaced by the following: 'ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6~~, other than ICT risks~~, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.' [...]'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the ESCB under the Treaty, ESCB members should keep the same level of involvement as currently provided for under the CSD Regulation as well as notifying the relevant authorities of ICT related incidents. The Eurosystem is the relevant authority for all euro area CSDs and for several other EU CSDs. ESCB central banks would need access to ICT-related incidents that are relevant to the performance of their duties, including the oversight of CSDs and other FMIs. The risks to which CSDs are exposed, including ICT risks, have the potential to threaten the sound functioning of CSDs. Therefore, ICT risks are of importance for relevant authorities, which should be provided with a full and detailed overview of these risks in order to assess them and influence the CSDs' risk management approach. In addition, the proposed regulation should not provide for less restrictive requirements as regards ICT risks when compared to those provided under the current CSD Regulation and related regulatory technical standards. See paragraph 2.2.3 of the ECB Opinion.*	

Drafting proposals in relation to a proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341

Amendment 1 Recitals (recital 4)	
'(4) In the area of banking services, Directive 2013/36/EU on access to the activity of credit institutions and the prudential regulation of credit institutions and investment firms currently sets out only general internal governance rules and operational risk provisions containing requirements for contingency and business continuity plans which implicitly serve as a basis for addressing ICT risk management. However, to ensure that ICT risk is explicitly addressed, the requirements for contingency and business continuity plans should be amended to include business continuity and disaster recovery plans also for ICT risk, in in accordance with the requirements laid down in Regulation (EU) 2021/xx [DORA].'	'(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~~ **that** ~~which implicitly~~ serve as a basis for addressing ICT risk management. ~~However, t~~**T**o ensure that ICT risk is explicitly addressed, **and Directive 2013/36/EU is fully coordinated** ~~the requirements for contingency and business continuity plans should be amended to include business continuity and disaster recovery plans also for ICT risk, in in accordance~~ with the requirements laid down in Regulation (EU) 2021/xx [DORA]**, the Directive's provisions on governance and operational risk should be amended.**'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities responsible for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, the ECB suggests that the recitals of the proposed amending directive be broadened and refer to Article 74 of the Capital Requirements Directive, which concerns robust governance arrangements. That is because the requirements under the proposed regulation go beyond contingency and business continuity plans. ICT risk governance measures, overall, fall under the more general scope of robust governance arrangements under Article 74 of the Capital Requirements Directive. See paragraph 3.6 of the ECB Opinion.*	
Amendment 2 Article 5	
'In Article 85 of Directive 2013/36/EU, paragraph 2 is replaced by the following:	'In Article 85 of Directive 2013/36/EU, ~~paragraph 2 is replaced by~~ the following **paragraph is added**:

'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.'	'**With reference to ICT ("information communication technology") risk,** ~~C~~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~~**also comply with the prudential requirements** 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.~~ .'
Explanation *In view of the close links between the provisions of the proposed regulation and the competences of the ECB and the national competent authorities responsible for the prudential supervision of credit institutions under the SSM Regulation and the Capital Requirements Directive, a clear renvoi from the Capital Requirements Directive to the proposed regulation should be provided to increase clarity and coordination between the proposed regulation and the Capital Requirements Directive. See paragraph 3.6 of the ECB Opinion.*	