COMMUNICATION FROM THE COMMISSION

Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)

(2023/C 328/02)

I. INTRODUCTION

1. Pursuant to Article 4(3) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), [1] the Commission shall, by 17 July 2023, provide guidelines clarifying the application of Article 4(1) and (2) of that Directive.

2. The present Guidelines clarify the application of those provisions, which concern the relationship between Directive (EU) 2022/2555 and current and future sector-specific Union legal acts addressing cybersecurity risk-management measures or incident reporting requirements. The Appendix to these Guidelines lists the sector-specific Union legal acts that the Commission considers to fall within the scope of Article 4 of Directive (EU) 2022/2555. The fact that an act is not listed in that Appendix does not necessarily mean that it does not fall within the scope of that provision.

3. In application of Article 4(3), third sentence, of Directive (EU) 2022/2555, the Commission took account of the observations of the NIS Cooperation Group and the European Union Agency for Cybersecurity (ENISA) prior to the adoption of the present Guidelines.

4. The present Guidelines are without prejudice to the interpretation of Union law by the Court of Justice of the European Union.

II. EQUIVALENCE OF CYBERSECURITY REQUIREMENTS OF SECTOR-SPECIFIC UNION LEGAL ACTS

5. Article 4(1) of Directive (EU) 2022/2555 provides that, where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in that Directive, the relevant provisions of Directive (EU) 2022/2555, including the provisions on supervision and enforcement laid down in Chapter VII of that Directive, shall not apply to such entities. That provision further provides that where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of Directive (EU) 2022/2555, the relevant provisions of that Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.

II.1. Cybersecurity risk-management requirements

6. Article 4(2)(a) of Directive (EU) 2022/2555 provides that cybersecurity risk-management measures that essential or important entities are required to adopt under sector-specific Union legal acts shall be considered to be equivalent in effect to the obligations laid down in Directive (EU) 2022/2555 where those measure are at least equivalent in effect to those laid down in Article 21(1) and (2) of that Directive. When assessing whether the requirements in a sector-specific Union legal act on cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2) of Directive (EU) 2022/2555, the requirements in that sector-specific Union legal act should, at a minimum, correspond to the requirements of those provisions or go beyond them, meaning that the sector-specific provisions may be more granular on substance compared to the corresponding provisions of Directive (EU) 2022/2555.

[1] OJ L 333, 27.12.2022, p. 80.

7. Pursuant to Article 21(1), first subparagraph, of Directive (EU) 2022/2555, Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services. Those measures should be risk-based and should be able to prevent or minimise the impact of incidents. Article 21(1), second subparagraph, of Directive (EU) 2022/2555 specifies how the proportionality of such measures should be assessed ([2]). The obligation laid down in Article 21(1) of Directive (EU) 2022/2555 requiring essential and important entities to take appropriate and proportionate cybersecurity risk-management measures refers to all operations and services of the entity concerned, not only to specific information technology ('IT') assets or critical services that the entity provides.

8. When assessing the equivalence of a sector-specific Union legal act with the relevant provisions on cyber risk-management of Directive (EU) 2022/2555, particular importance should be given in that assessment to the question whether the security obligations in that legal act comprise measures aiming to ensure the security of network and information systems. The definition of 'security of networks and information systems' laid down in Article 6, point (2) of Directive (EU) 2022/2555 refers to the ability of information systems to resist, at a given level of confidence, any event that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or of services offered by, or accessible via, those network and information systems. The use of the terms 'availability', 'authenticity', 'integrity' and 'confidentiality' in that definition refers to all four protection goals related to the security of network and information systems. The term 'network and information systems', as defined in Article 6, point (1) of Directive (EU) 2022/2555, encompasses electronic communication networks ([3]); any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; and digital data stored, processed, retrieved or transmitted by such electronic communication networks or devices for the purposes of their operation use, protection or maintenance. Consequently, the security measures required by a sector-specific Union legal act should also cover hardware, firmware, and software used in the activities of an entity.

9. Another important consideration when assessing the equivalence of a sector-specific Union legal act with the requirements of Article 21(1) and (2) of Directive (EU) 2022/2555 is that the cybersecurity risk-management measures required by that act should be based on an 'all-hazard approach'. Since threats to the security of network and information systems could have different origins, any type of event can have a negative impact on the network information systems of the entity and potentially lead to an incident. Therefore, the cybersecurity risk-management measures taken by the entity should protect not only the entity's network and information systems, but also the physical environment of those systems from any event such as sabotage, theft, fire, flood, telecommunication or power failures, or unauthorised physical access that are capable of compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. Consequently, the cybersecurity risk-management measures required by a sector-specific Union legal act should specifically address the physical and environmental security of network and information systems from systems failure, human error, malicious acts, or natural phenomena ([4]).

10. Article 21(2) of Directive (EU) 2022/2555 further requires the cybersecurity risk-management measures to include the specific security requirements listed in lit (a) to (j) of paragraph 2 of that provision. Those requirements cover measures such as policy on risk-analysis and information system security, incident handling, business continuity, crisis-management, supply chain security, policies and procedure regarding the use of cryptography, and where appropriate, encryption. Pursuant to Article 21(5), second subparagraph, of Directive (EU) 2022/2555, the Commission is empowered to adopt implementing acts laying down the technical and methodological requirements, as well as sectorial requirements, as necessary, of the security measures referred to in Article 21(2) of

([2]) See also recitals 78, 81 and 82 of the preamble to Directive (EU) 2022/2555.

([3]) Article 2(1) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

([4]) See Recital 79 of the preamble to Directive (EU) 2022/2555.

that Directive. With regard to Domain Name System ('DNS') service providers, top-level Domain ('TLD') name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, the Commission shall adopt, by 17 October 2024, implementing acts on the technical and methodological requirements of the security measures referred to in Article 21(2) of Directive (EU) 2022/2555. Implementing acts specify in further detail the main conditions and criteria for implementation as laid down in the basic act, without affecting the substance of that act ([5]).

II.2. **Reporting requirements**

11. Article 4(2)(b) of Directive (EU) 2022/2555 provides that reporting requirements concerning the notification of significant incidents shall be considered to be equivalent in effect to the obligations of that Directive where a sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the computer security incident response teams ('CSIRTs'), the competent authorities, or the single points of contact ('SPOCs'), and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of Directive (EU) 2022/2555.

12. Since the requirements of a sector-specific Union legal act to notify significant incidents must be at least equivalent in effect to those laid down in Article 23(1) to (6) of Directive (EU) 2022/2555 for that act to apply instead of the reporting obligations of that Directive, the requirements laid down in Article 23(1) to (6) of the Directive are of particular importance for the assessment of equivalence. Article 23(1) to (6) of Directive (EU) 2022/2555 prescribe in more detail what kind of incidents must be reported to whom, in what timeframe, and with what information content. This is explained in more detail in the following subsections:

II.2.1. *Notification of significant incidents to CSIRTs, competent authorities and recipients*

13. The first sentence of Article 23(1), first subparagraph, of Directive (EU) 2022/2555 requires essential and important entities to notify, without undue delay, its CSIRT or, where applicable, its competent authority, of any significant incident. The second sentence of Article 23(1), first subparagraph, of Directive (EU) 2022/2555 requires essential and important entities to notify, where appropriate, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services.

14. While Article 6, point (6), of Directive (EU) 2022/2555 defines 'incidents' very broadly, as any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, Article 23(1) of that Directive only subjects significant incidents to a reporting obligation. An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned (Article 23(3)(a)) or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage (Article 23(3)(b)).

([5]) See Chapter D Additional Rules Implementing the Basic Act, Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union — 18 June 2019 (OJ C 223, 3.7.2019, p. 1).

15. Recital (101) of the preamble to Directive (EU) 2022/2555 clarifies that the reporting of incidents should be based on an initial assessment carried out by the entity concerned. Such an initial assessment should consider, inter alia, the affected network and information systems, in particular their importance in the provision of the entity's services, the severity and technical characteristics of a cyber threat, and any underlying vulnerabilities that are being exploited, as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident, or the number of affected recipients of services may play an important role in identifying whether the operational disruption of the service is severe.

16. Pursuant to Article 23(11), second subparagraph, of Directive (EU) 2022/2555, the Commission is empowered to adopt implementing acts further specifying the cases in which an incident shall be considered significant. With regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, the Commission shall adopt, by 17 October 2024, such implementing acts. Implementing acts specify in further detail the main conditions and criteria for implementation as laid down in the basic act, without affecting the substance of that act ([6]).

II.2.2. *Multiple-stage approach to and time frame for reporting significant incidents*

17. Directive (EU) 2022/2555 lays down a multiple-stage approach to the reporting of significant incidents which entails an early warning, an incident notification, and a final report. These three elements may possibly be supplemented by intermediate reports and a progress report.

18. The multiple-stage approach aims at striking the right balance between, on one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows essential and important entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual entities and entire sectors ([7]).

19. According to the multiple-stage approach, essential and important entities must first submit an early warning, without undue delay and in any event within 24 hours of becoming aware of the significant incident, to the competent CSIRT or authority. Subsequently, those entities must submit an incident notification, without undue delay and in any event within 72 hours of becoming aware of the significant incident. Thereafter, an intermediate report may be requested by a competent CSIRT or authority. Finally, a final report must be provided to the competent CSIRT or authority not later than one month after the submission of the incident notification, unless the incident is still ongoing at that time, in which case a progress report must be provided and the final report within one month of the handling of the incident.

20. A different timeframe applies for the incident notification laid down in Article 23(4), second subparagraph, of Directive (EU) 2022/2555 in relation to trust service providers. Those providers must notify significant incidents on the provision of their trust services without undue delay and in any event within 24 hours of becoming aware of the significant incident.

([6]) See Chapter D Additional Rules Implementing the Basic Act, Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union — 18 June 2019, (OJ C 223, 3.7.2019, p. 1).

([7]) See Recital 101 of the preamble to Directive (EU) 2022/2555.

II.2.3. *Content of reporting obligation of significant incidents to CSIRTs or competent authorities*

21. As a general rule, the third sentence of Article 23(1), first subparagraph, of Directive (EU) 2022/2555 requires Member States to ensure that essential and important entities report, inter alia, any information enabling the competent CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. This requirement concerning the content of the reporting obligation is further specified in Article 23(4) of Directive (EU) 2022/2555, which lays down the multiple-stage approach.

22. According to Article 23(4)(a), the early warning must include, where applicable, an indication whether the significant incident is suspected of being caused by unlawful or malicious acts or if it could have (in terms of whether it is likely to have) a cross-border impact. According to recital (102) of the preamble to Directive (EU) 2022/2555, the early warning should only include the information necessary to make the competent CSIRT or authority aware of the significant incident and to allow the entity concerned to seek assistance, if required.

23. The incident notification must include, where applicable, updates to the information submitted as part of the early warning. Moreover, it must include an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise.

24. In case an intermediate report is requested, it must include relevant status updates. The final report must include a detailed description of the incident, including its severity and impact, the type of threat or root cause that is likely to have triggered the incident, the applied and ongoing mitigation measures, and, where applicable, the cross-border impact of the incident.

II.2.4. *Immediate access to incident notifications*

25. Article 4(2)(b) of Directive (EU) 2022/2555 provides that a sector-specific Union legal act, to be applicable with regard to the notification requirements instead of that Directive, needs to provide the CSIRTs, the competent authorities, or the SPOCs under Directive (EU) 2022/2555 with immediate access to the incident notifications submitted in accordance with the sector-specific Union legal act. In accordance with Recital (24) of the preamble to Directive (EU) 2022/2555, such immediate access can be ensured, in particular, if incident notifications are being forwarded without undue delay to the CSIRT, the competent authority, or the SPOC.

26. Immediate access may be provided through automatic and direct means which Member States should put in place, where appropriate. Automatic and direct reporting mechanisms ensure systematic and immediate sharing of information with the CSIRTs, the competent authorities, or the SPOCs concerning the handling of incident notifications. Member States may also use a single entry point which needs to comply with the sector-specific Union legal act, to simplify reporting and to implement the automatic and direct reporting mechanism.

27. When assessing whether the requirements in a sector-specific Union legal act to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of Directive (EU) 2022/2555, the requirements in that sector-specific Union legal act should, at a minimum, correspond to the requirements of Article 23(1) to (6) or provide for greater detail than those provisions. The requirements should relate to the kind of incidents that need to be reported according to Directive (EU) 2022/2555, taking into account in particular the recipients, the content, and the applicable time frames.

III. CONSEQUENCES OF EQUIVALENCE

III.1. Supervision and enforcement

28. Where sector-specific Union legal acts are at least equivalent in effect to the obligations laid down in Directive (EU) 2022/2555, it is not only the relevant provisions of that Directive concerning the obligation to adopt cybersecurity risk-management measures or to notify significant incidents that do not apply, but also the provisions on supervision and enforcement laid down in Chapter VII of Directive (EU) 2022/2555.

29. Recital (25) of the preamble to Directive (EU) 2022/2555 explains that sector-specific Union legal acts that are at least equivalent in effect could provide that the competent authorities under those acts exercise their supervisory and enforcement powers in relation to cybersecurity risk-management or notification obligations with the assistance of the competent authorities under Directive (EU) 2022/2555. The competent authorities concerned could establish cooperation arrangements for that purpose, including procedures concerning the coordination of supervisory activities, procedures on investigations and on-site inspections in accordance with national law, and a mechanism for the exchange of relevant information on supervision and enforcement between the competent authorities. Such a mechanism for the exchange of relevant information could entail the access to cyber-related information requested by the competent authorities under Directive (EU) 2022/2555.

III.2. National cybersecurity strategy

30. Each Member State is required to adopt a national cybersecurity strategy pursuant to Article 7(1) of Directive (EU) 2022/2555. A national cybersecurity strategy is a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve those objectives and priorities in that Member State (see Article 6, point (4), of Directive (EU) 2022/2555). The cybersecurity strategy must include inter alia objectives and priorities covering in particular the sectors referred to in Annexes I and II to Directive (EU) 2022/2555. In addition, that strategy must entail a governance framework to achieve those objectives and priorities, including the policies referred to in Article 7(2) of Directive (EU) 2022/2555.

31. Moreover, Article 7(1)(c) of Directive (EU) 2022/2555 provides that the national cybersecurity strategy must include a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the SPOCs and the CSIRTs under Directive (EU) 2022/2555, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts.

32. Hence, the requirement for adopting a cybersecurity strategy pursuant to Article 7 of Directive (EU) 2022/2555 neither concerns the cybersecurity requirements imposed on essential and important entities pursuant to Articles 21 and 23 of that Directive, nor the provisions related to their supervision and enforcement laid down in Chapter VII as required by Article 4(1) and (2) of the Directive. The relevant provision of Article 7 should continue to apply with respect to sectors, subsectors and types of entities for which sector-specific Union legal acts within the meaning of Article 4 of Directive (EU) 2022/2555 exist.

III.3. Designation of CSIRTs

33. According to Article 10(1) of Directive (EU) 2022/2555, Member States must designate or establish one or more CSIRTs which shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II of the Directive, thus including the sectors, subsectors and types of entities for which sector-specific Union legal acts exist. CSIRTs will normally also carry out their tasks as laid down in Article 11(3) of Directive (EU) 2022/2555 in that regard, unless particular tasks are specified in the sector-specific Union legal acts.

III.4. **National cyber crisis management frameworks and EU-CyCLONe**

34. Pursuant to Article 9(1) of Directive (EU) 2022/2555, the Member States must designate or establish one or more cyber crisis management authorities who are responsible for the management of large-scale cybersecurity incidents and crises. According to Article 6, point (7), of that Directive, a large-scale cybersecurity incident is an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States. Article 9(4) of Directive (EU) 2022/2555 requires the Member States to also adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. This plan should lay down, inter alia, the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels, and the relevant public and private stakeholders and infrastructure involved. Such cyber crisis management procedures and relevant public and private stakeholders and infrastructure might involve sector-specific procedures and stakeholders.

35. Article 16 of Directive (EU) 2022/2555 establishes the European cyber crisis liaison organization network (EU-CyCLONe), whose purpose is to support the coordinated management of large-scale cybersecurity incidents and crisis at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies.

36. Since Article 9 on cyber crisis management frameworks and Article 16 on EU-CyCLONe do not concern the cybersecurity requirements imposed on entities pursuant to Article 21 and 23 of Directive (EU) 2022/2555 or the supervision and enforcement laid down in Chapter VII as required by Article 4(1) and (2) of that Directive, Article 9 and 16 should apply in their entirety for sectors, despite the existence of sector-specific Union legal acts within the meaning of Article 4. As a result, Member States must designate or establish one or more cyber crisis management authorities responsible for the management of large-scale cybersecurity incidents and crises occurring in the sectors covered by sector-specific Union legal acts. Furthermore, sectors covered by sector-specific Union legal acts should not be disregarded when adopting the national large-scale cybersecurity incident and crisis response plan. Finally, EU-CyCLONe should carry out its tasks enshrined in Article 16 of Directive (EU) 2022/2555 with regard to sectors where entities are subject to sector-specific Union legal acts.

III.5. **Exclusion of the application of Articles 3 (3) and (4), 20 and 27 (2) and (3)**

37. Pursuant to Article 3(3) of Directive (EU) 2022/2555, Member States are required to establish a list of essential and important entities as well as entities providing domain name registration services falling under the scope of the Directive. Pursuant to Article 27 (2), Member States shall require entities referred to in Article 27 (1) of that Directive to submit certain information to the competent authorities. Since the purpose of these provisions is to ensure a clear overview of the entities falling within the scope of Directive (EU) 2022/2555 to support the supervision of essential and important entities falling under its scope, it follows that these provisions should not apply to entities for which a sector-specific Union legal act applies with respect to cybersecurity risk-management and reporting requirements. This does not preclude Member States from including such entities in the list.

Pursuant to Article 20(1) of Directive (EU) 2022/2555, management bodies of essential and important entities are required to approve the cybersecurity risk-measures taken by those entities in order to comply with Article 21, oversee its implementation, and can be held liable for infringements by the entities of that Article. Pursuant to Article 20(2) of that Directive, Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. Since the obligations stemming from Article 20 of Directive (EU) 2022/2555 are intrinsically linked to the requirements of Article 21 of that Directive, it follows that Article 20 should not apply in the case of sector-specific Union legal acts within the meaning of Article 4 of that Directive applying with respect to cybersecurity risk-management requirements.

APPENDIX

Sector-specific Union legal acts

Regulation (EU) 2022/2554 (Digital Operational Resilience Act) [1]

1. Article 1(2) of the Regulation (EU) 2022/2554 (Digital Operational Resilience Act, DORA) provides that, in relation to financial entities covered by Directive (EU) 2022/2555 and its corresponding national transposition rules, Regulation (EU) 2022/2554 shall be considered a sector-specific Union legal act for the purposes of Article 4 of Directive (EU) 2022/2555. This statement is mirrored in recital (28) of the preamble to Directive (EU) 2022/2555, which says that DORA should be considered a sector-specific Union legal act in relation to Directive (EU) 2022/2555 with regard to financial entities. Consequently, the provisions of Regulation (EU) 2022/2554 relating to information and communication technology (ICT) risk management (Article 6 et seq.), management of ICT-related incidents and, in particular, major ICT-related incident reporting (Article 17 et seq.), as well as on digital operational resilience testing, (Art 24 et seq.) information-sharing arrangements (Article 25) and ICT third-party risk (Article 28 et seq.) shall apply instead of those provided for in Directive (EU) 2022/2555. Member States should therefore not apply the provisions of Directive (EU) 2022/2555 on cybersecurity risk-management and reporting obligations, and supervision and enforcement, to financial entities covered by Regulation (EU) 2022/2554.

2. In this regard, financial entities are considered entities referred to in Article 2(1)(a) to (t) of Regulation (EU) 2022/2554. The types of entities that fall within the scope of Regulation (EU) 2022/2554 as financial entities, as well as within the scope of Directive (EU) 2022/2555 as essential or important entities, include credit institutions, trading venues and central counterparties. Since it is important to maintain a strong relationship and the exchange of information with the financial sector under Directive (EU) 2022/2555, the European Supervisory Authorities and the competent authorities under Regulation (EU) 2022/2554 may request to participate in the activities of the Cooperation Group [2], and exchange information and cooperate with the SPOCs, as well as with the CSIRTs and the competent authorities under Directive (EU) 2022/2555 [3]. The competent authorities under Regulation (EU) 2022/2554 should also transmit details of major ICT-related incidents and, where relevant, significant cyber threats to the CSIRTs, the competent authorities, or the SPOCs under Directive (EU) 2022/2555. This may be achieved by providing immediate access to incident notifications and forwarding them either directly or through a single entry point. CSIRTs should be in a position to cover the financial sector in their activities [4]. Member States should continue to include the financial sector in their cybersecurity strategies. The provisions on national cyber crisis management frameworks (Article 9 of Directive (EU) 2022/2555), as well as on EU-CyCLONe (Article 16 of Directive (EU) 2022/2555), should continue to apply to entities falling within the scope of Regulation (EU) 2022/2554.

---

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

[2] Article 14(3) of Directive (EU) 2022/2555 and Article 47(1) of Regulation (EU) 2022/2554.

[3] See Recital 28 of Directive (EU) 2022/2555.

[4] Ibid.