Official Journal
of the European Union

EN
L series

2025/299

13.2.2025

COMMISSION DELEGATED REGULATION (EU) 2025/299

of 31 October 2024

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulation (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ([1]), and in particular Article 68(10), third subparagraph, thereof,

Whereas:

(1) Articles 11 and 12 of Regulation (EU) 2022/2554 of the European Parliament and of the Council ([2]) provide for requirements relating to response and recovery, backup policies and procedures, restoration and recovery procedures and methods concerning the ICT systems of financial entities, including crypto-asset services providers. Commission Delegated Regulation (EU) 2024/1774 ([3]) further specifies components of the ICT business continuity policy, the testing of ICT business continuity plans, the components of the ICT response and recovery plans of financial entities, including crypto-asset service providers. This Regulation complements those provisions of Regulation (EU) 2022/2554 and of Delegated Regulation (EU) 2024/1774 with respect to continuity and regularity in the performance of the crypto-asset services.

(2) In providing their services, crypto-asset service providers may use a distributed ledger over which they have no control, including a permissionless distributed ledger. In that case, they may not be capable of ensuring the regularity and continuity of their services when disruptions are caused by problems that are inherent to the operation of such distributed ledgers. To mitigate market volatility that may have an adverse impact on clients affected by such disruptions, crypto-asset service providers should include in their business continuity policy measures for timely communication with clients and other external stakeholders. Such communication should include essential and timely information for clients on such disruptions, including ongoing status updates, until the disruption is resolved and services are resumed. Where information on the status of the permissionless distributed ledger responsible for a service disruption is not readily available to the crypto-asset service provider, that crypto-asset service provider should communicate updates to clients and other stakeholders, including competent authorities, on a best effort basis to ensure that clients and stakeholders have as comprehensive information as possible on such disruptions.

([1]) OJ L 150, 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([3]) Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (OJ L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj).

(3) To avoid disproportionate administrative burden for small and medium-enterprises and start-ups, crypto-asset service providers should consider in their business continuity policy the scale, nature, and range of the services they provide. That means that crypto-asset service providers should determine their specific business continuity requirements on the basis of a robust self-assessment, based on a number of criteria that would enable them to implement a business continuity policy that is commensurate with the market impact of their services. The self-assessment should also take into account other circumstances beyond those listed in the Annex that may have an impact on the crypto-asset service provider.

(4) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority.

(5) The European Securities and Markets Authority has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([4]),

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(a) 'critical or important function' means a critical or important function as defined in Article 3, point (22), of Regulation (EU) 2022/2554;

(b) 'permissionless distributed ledger' means a specific type of distributed ledger in which no entity controls the distributed ledger and DLT network nodes can be set up by any person complying with the technical requirements and the protocols of that distributed ledger.

Article 2

Business continuity organisational arrangements

1. The business continuity policy referred to in Article 68(7) of Regulation (EU) 2023/1114 shall be comprised of plans, procedures and measures.

2. The management body of crypto-asset service providers, in the exercise of its functions referred to in Article 68(6) of Regulation (EU) 2023/1114, shall establish and endorse the plans, procedures, and measures that comprise the business continuity policy. The crypto-asset service provider's management body shall be responsible for the implementation of the business continuity policy, and for reviewing its effectiveness at least on an annual basis.

3. Crypto-asset service providers shall ensure that any modifications to the business continuity policy are transmitted to all relevant internal staff through effective communication channels.

([4]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

Article 3

Business continuity policy

1. The business continuity policy referred to in Article 68(7) of Regulation (EU) 2023/1114 shall ensure that crypto-asset service providers properly address disruptive incidents or performance issues relating to the systems critical to the operation of their business functions and it shall be laid down in a durable medium.

2. Crypto-asset service providers shall include in the business continuity policy all of the following:

(a) a specification of the scope of the business continuity policy, including its limitations and exclusions, to be covered by the business continuity plans, procedures, and measures;

(b) a description of the criteria to activate the business continuity plans, including escalation procedures up to the level of the management body;

(c) provisions on the governance and organisation of the crypto-asset service provider, including, the roles and responsibilities of the staff, ensuring that sufficient resources are available for the effective implementation of the policy;

(d) provisions that ensure consistency between the business continuity plans and the ICT-business continuity plans, and ICT response and recovery plans referred to in Articles 24 and 26 of Delegated Regulation (EU) 2024/1774.

Article 4

Business continuity plans

1. When implementing the business continuity policy referred to in Article 68(7) of Regulation (EU) 2023/1114, crypto-asset service providers shall establish business continuity plans. The business continuity plans shall set out the procedures necessary to protect and, where necessary, re-establish:

(a) the confidentiality, integrity, and availability of client data;

(b) the availability of the business functions, supporting processes and information assets of the crypto-asset service providers.

2. The business continuity plans shall contain the following:

(a) a range of possible adverse scenarios relating to the operation of critical or important functions, including the unavailability of business functions, staff, workspace, external suppliers, data centres, or loss or alteration of critical data and documents;

(b) the procedures and policies to be followed in case of a disruptive incident, including:

  (i) the measures that are necessary to recover critical or important functions;

  (ii) the deadlines by which those critical or important functions are to be recovered;

  (iii) recovery point objectives;

  (iv) the maximum time to resume services;

(c) the procedures and policies for relocating the business functions used to provide crypto-asset services to a back-up site;

(d) back-up of critical business data, including up-to-date information of the necessary contacts to ensure communication inside the crypto-asset service provider, between the crypto-asset service provider and its clients;

(e) procedures for timely communications with clients and other external stakeholders, including competent authorities.

3. In the event of a disruption involving a permissionless distributed ledger used by the crypto asset service provider in the provision of its services, the communications referred to in paragraph 2, point (e) shall include the following information:

(a) when the services are expected to be resumed;

(b) the reasons and the impact of the disruptive incident;

(c) any risks concerning clients' funds and crypto-assets held on their behalf;

(d) measures that the crypto-asset service intends to take in response to the disruption of a permissionless distributed ledger.

Where that information is not readily available to the crypto-asset service provider, the crypto-asset service provider shall communicate updates as regards the information in the first subparagraph to clients and stakeholders, including competent authorities, on a best effort basis.

4. The business continuity plans shall contain procedures to address any disruptions of outsourced critical or important functions, including where those critical or important functions become unavailable.

Article 5

Periodic testing of the business continuity plans

1. Crypto-asset service providers shall test the operation of the business continuity plans referred to in Article 4 on the basis of realistic scenarios. Such testing shall verify the capability of the crypto-asset service provider to recover from disruptive incidents and to resume services in accordance with Article 4(2), point (b).

2. Crypto-asset service providers shall test the business continuity plans annually taking into account:

(a) the results of the tests referred to in paragraph 1;

(b) the most recent threat intelligence;

(c) lessons derived from previous events;

(d) where relevant, any changes in the recovery objectives, including recovery time objectives and recovery point objectives as referred to in Article 4(2), point (b);

(e) changes in the business functions.

3. Crypto-asset service providers shall document the results of the testing activity in writing, and submit them to their management body and to the operating units involved in the business continuity plans.

4. Crypto-asset service providers shall ensure that the testing of the business continuity plans does not interfere with normal conduct of their services.

Article 6

Complexity and risk considerations

1. When establishing the business continuity policy, including the plans, procedures and measures, crypto-asset service providers shall take into account elements of increased complexity or risk, including:

(a) the type and range of crypto-asset services offered;

(b) the extent to which the services of the crypto-asset service provider rely on permissionless distributed ledger;

(c) the potential impact of any disruptions on the continuity of the crypto-asset service provider's activities and availability of its services.

2. For the purposes of paragraph 1, crypto-asset service providers shall conduct a self-assessment of the scale, the nature, and range of their services annually. Crypto-asset service providers shall base that self-assessment on the criteria set out in the Annex and any other criteria that the crypto-asset service provider considers relevant.

Article 7

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 31 October 2024.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

CRITERIA FOR THE SELF-ASSESSMENT OF CRYPTO-ASSET SERVICE PROVIDERS

(a) The nature of the crypto-asset service provider, based on the following elements:

  (i) the class designation referred to in Annex IV to Regulation (EU) 2023/1114;

  (ii) the average liquidity levels, or market depth, of crypto-assets available to trade on a trading platform for crypto-assets, where applicable;

  (iii) the role of the crypto-asset service provider in the financial system, including whether the crypto-asset service provider operates a trading platform for crypto assets and whether crypto-assets traded on its platform are traded on other trading platforms for crypto-assets.

(b) Scale, by assessing the impact of the crypto-asset service provider on the orderly functioning of the markets based on the following elements, where applicable:

  (i) whether the crypto-asset service provider qualifies as significant as referred to Article 85 of Regulation (EU) 2023/1114;

  (ii) the number of countries in which the crypto-asset service provider is conducting business activity;

  (iii) the number of clients;

  (iv) the number of active users;

  (v) the value of crypto-assets held in custody;

  (vi) the volume of transactions on a trading platform for crypto-assets;

  (vii) the number of transfers of crypto-assets conducted on behalf of clients;

  (viii) the number of orders executed on behalf of clients.

(c) Complexity, by assessing the following elements, where applicable:

  (i) the structure of the crypto-asset service provider in terms of ownership and governance, and its organisational, operational, technical, physical, and geographical presence;

  (ii) the level of outsourcing of the crypto-asset service provider, and in particular whether any critical or important operational functions have been outsourced;

  (iii) the number and type of distributed ledgers used in the execution of services;

  (iv) the number of DLT network nodes the crypto-asset service provider operates on one or multiple distributed ledger(s);

  (v) the number and type of smart contracts deployed and maintained by the crypto-asset service provider;

  (vi) how the private cryptographic keys of clients or other means of accessing crypto-assets are secured under safekeeping;

  (vii) the use of software and hardware-based custodial wallets or wallets that secure cryptographic keys using multiple fiduciaries.

For the purposes of points (b)(iii) to (viii), the crypto-asset service provider shall use for the self-assessment the daily average over a one-year reference period.