GLOBAL FORUM ON
TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

Delivering Tax Transparency to Crypto-Assets: A Step-by-Step Guide to Understanding and Implementing the Crypto-Asset Reporting Framework

OECD
BETTER POLICIES FOR BETTER LIVES

Delivering Tax Transparency to Crypto-Assets: A Step-by-Step Guide to Understanding and Implementing the Crypto-Asset Reporting Framework

BETTER POLICIES FOR BETTER LIVES

This guide was approved by the Crypto-Asset Reporting Framework (CARF) Group on 4 October 2024 and adopted via written procedure by the Global Forum Plenary on 9 November 2024. It was prepared for publication by the Secretariat of the Global Forum.

Please cite this document as:

OECD (2024), *Delivering tax transparency to Crypto-Assets: A step-by-step guide to understanding and implementing the Crypto-Asset Reporting Framework*, Global Forum on Transparency and Exchange of Information for Tax Purposes, OECD, Paris, https://www.oecd.org/tax/transparency/documents/step-by-step-guide-understanding-implementing-crypto-asset-reporting-framework.pdf.

Photo credits: OECD with cover illustration by Renaud Madignier

Table of contents

Introduction and overview

Introduction and background

1. The growth in the Crypto-Asset sector provides a variety of new business opportunities, including for innovation and investment. Notwithstanding that, the growth in the use of Crypto-Assets should not be at the expense of transparency for tax purposes. There are several factors associated with Crypto-Assets that present significant new risks to tax transparency and that could reverse the recent global gains in this area. Firstly, the Crypto-Asset market is characterised by a shift away from traditional financial intermediaries, the typical information providers in third-party tax reporting regimes, including the Standard in the Automatic Exchange of Financial Account Information in Tax Matters (commonly referred to as the Common Reporting Standard, or CRS[1]), to a new set of service providers which, to date, have often not been the focus of financial regulation and that have frequently not yet been subject to tax reporting requirements with respect to their users. Secondly, these service providers may have no physical headquarters or other conventional business presence and instead carry out their activities entirely online, making them more difficult to identify and locate than traditional financial institutions. In operating this way, these service providers can also change the jurisdictions in which they carry out their activities in a rapid and non-transparent manner. Similarly, investors in Crypto-Assets may carry out their activities entirely online without being required to provide information about their identity or can hold Crypto-Assets in personal devices that are known only to that Crypto-Asset User. Accordingly, residents of a jurisdiction may be engaging in Crypto-Asset transactions giving rise to tax liabilities or investing in Crypto-Assets without the knowledge of tax administrations. Thirdly, the ability of individuals to hold Crypto-Assets in wallets (i.e. accounts for holding Crypto-Assets) unaffiliated with any service provider and to transfer such Crypto-Assets between jurisdictions, presents the risk that Crypto-Assets are used for illicit activities or to evade tax obligations.

2. Overall, these characteristics of the Crypto-Asset sector limit the visibility of tax authorities over tax-relevant activities of their taxpayers that are carried out within the sector, increasing the difficulty for tax authorities to verify whether any associated tax liabilities are being appropriately reported and assessed. This is reflected in the growth of the Crypto-Asset sector being identified by the Global Forum's Task Force on Risk as one of the top risks to tax transparency. Similarly, the risks associated with the growth in the Crypto-Asset sector have been identified in the context of global anti-money laundering efforts, whereby the Financial Action Task Force (FATF) has developed a set of recommendations and guidance with respect to the measures that should be in place for Virtual Asset Service Providers.[2]

3. To address the risks posed by Crypto-Assets with respect to transparency for tax purposes, in June 2023, the OECD, working with G20 countries, completed and published the Crypto-Asset Reporting

[1] Standard for Automatic Exchange of Financial Account Information in Tax Matters: https://www.oecd.org/en/publications/standard-for-automatic-exchange-of-financial-account-information-for-tax-matters_9789264216525-en.html

[2] FATF, Virtual Assets: https://www.fatf-gafi.org/en/topics/virtual-assets.html

Framework (CARF).[3] This framework provides for the reporting and automatic exchange of information (AEOI) in relation to Crypto-Assets between tax authorities for tax compliance purposes. G20 Leaders immediately welcomed the development and invited the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) to support the rapid and widespread implementation of the CARF.[4] In anticipation of the completion of the work and recognising the benefits of the CARF, the Global Forum agreed, at its 2022 Plenary meeting, to build on its commitment and monitoring processes to ensure the widespread implementation of the CARF.[5] Furthermore, as part of a jurisdiction-led commitment process demonstrating the political momentum behind the implementation of the CARF, 59 jurisdictions have adhered to a Joint Statement stating their intent to work towards implementing the CARF in time to commence exchanges under the CARF in 2027.[6]

4. The Global Forum has since completed its work to develop its CARF commitment process, designed to ensure an effective CARF based on a level playing field. By the time of 2024 Global Forum Plenary meeting, around 60 jurisdictions had committed to implement the CARF in time to commence exchanges under the CARF in 2027, or 2028, where they face particular challenges with the 2027 timeline.

This Guide – supporting the delivery of the commitments to the CARF

5. This Step-by-Step Guide is intended to facilitate further commitments by jurisdictions to implement the CARF to ensure its widespread implementation, as well as to help support the implementation of the CARF thereafter, by raising the awareness of jurisdictions and the private sector in relation to what making such a commitment entails and the steps that must be taken in order to implement the CARF on a consistent basis and in accordance with the requirements.

6. Although each jurisdiction's specific approach will vary depending on its own unique circumstances, implementing the CARF involves several key building blocks that jurisdictions will need to consistently put in place. Such consistency in approach to CARF implementation is needed to ensure a level playing field across jurisdictions, minimise the reporting and information exchange burden for both the obliged service providers under the CARF (i.e. Reporting Crypto-Asset Service Providers (RCASPs[7])) as well as tax authorities, and, crucially, optimise the effective use of the CARF information exchanged. Specifically, the CARF building blocks involve jurisdictions:

---

[3] In this document, all references to the "CARF" include the CARF rules and the Commentary to the CARF, as well as the CARF Multilateral Competent Authority Agreement (CARF MCAA) and the Commentary to the CARF MCAA. See, International Standards for Automatic Exchange of Information in Tax Matters - Crypto-Asset Reporting Framework and 2023 updates to the Common Reporting Standard, 8 June 2023: https://www.oecd.org/tax/international-standards-for-automatic-exchange-of-information-in-tax-matters-896d79d1-en.htm

[4] G20 New Delhi Leaders' Declaration, 9-10 September 2023, paragraph 62: https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf.

[5] Statement of Outcomes of the 2022 Global Forum Plenary Meeting, 9-11 November 2022; available at: Statement of Outcomes 2022 Global Forum plenary meeting (oecd.org).

[6] Joint Statement on the implementation of the CARF: Joint Statement on the Implementation of the Crypto-Asset Reporting Framework (CARF) (oecd.org)

[7] The term "Reporting Crypto-Asset Service Provider" means any individual or Entity that, as a business, provides a service effectuating Exchange Transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary, to such Exchange Transactions, or by making available a trading platform. See, Section IV.B(1), International Standards for Automatic Exchange of Information in Tax Matters - Crypto-Asset Reporting Framework and 2023 updates to the Common Reporting Standard, 8 June 2023: https://www.oecd.org/tax/international-standards-for-automatic-exchange-of-information-in-tax-matters-896d79d1-en.htm

- making a political commitment to conduct CARF exchanges from a specified date;
- implementing legal frameworks covering both domestic and international aspects;
- adopting an administrative and Information Technology (IT) framework to ensure compliance and to support the exchanges operationally; and
- ensuring appropriate confidentiality safeguards are in place.

7. Furthermore, private sector actors will need to invest resources to understand, plan for and carry out their obligations to jurisdictions that have implemented the CARF. The steps they will need to carry out include:

- determining whether the private sector actor is a RCASP;
- determining which jurisdictions the RCASP has a nexus to under the rules implemented by the jurisdictions consistent with the CARF, and, therefore, which jurisdiction the RCASP will report to;
- understanding the due diligence and reporting obligations in the reporting jurisdiction and the procedures and systems that will be needed to fulfil them; and
- implementing the requirements to ensure the effective implementation of the customer due diligence and reporting obligations.

8. For jurisdictions and Financial Institutions that have implemented the CRS, which provides for AEOI in relation to Financial Accounts, many of these steps are familiar. As will be outlined throughout this document, the approaches to implement these building blocks can often build directly on the approaches used to implement the CRS.

9. This document is therefore intended to provide a starting point for governmental authorities and relevant private sector actors to understand each of these aspects in relation to the implementation of the CARF. The objective is to thereby ensure that all stakeholders are informed about what implementing the CARF entails, as well as to support a harmonised approach with respect to its implementation. Note that this document is not intended to interpret, add to, or alter the CARF and is without prejudice to a jurisdiction's domestic implementing legislation or rules consistent with the CARF. In the event that there is any discrepancy or lack of clarity regarding the contents of this document and the CARF, the CARF shall prevail. Furthermore, RCASPs should not rely on the contents of this document to satisfy themselves that they are complying with the requirements of the CARF. Instead, RCASPs must refer to the implementation of the requirements in the jurisdiction(s) in which they are subject to due diligence and reporting obligations, in order to ensure the requirements are complied with in that jurisdiction.

Overview of the Crypto-Asset Reporting Framework

10. The CARF provides for AEOI in relation to Crypto-Assets. The CARF defines "Crypto-Assets" as "a digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions", which includes cryptocurrencies, as well as cryptography-based tokens. This definition is intentionally broad, as the market for Crypto-Assets continues to develop rapidly. Recent years have witnessed increasing popularity, transactions in and the value of a number of Crypto-Asset types, attracting professional investors, as well as individuals, to the sector. Unlike traditional currencies issued by governments, Crypto-Assets rely on new technologies (i.e. cryptography and distributed ledger technology) that allow for the issuing, recording, transferring and storing of Crypto-Assets in a decentralised manner, without the need to rely on traditional financial intermediaries or a centralised administrator (e.g. a central bank or government authority). Crypto-Assets can also be used to make payments for goods and services, again without the need to rely on traditional financial intermediaries. Many users are attracted by the decentralised nature of Crypto-Assets, which can allow for them to be sent across national borders faster, more cheaply and more easily than traditional currency issued by

governments and financial assets and offer potentially novel forms of investment. The CARF is therefore designed to apply to such activities, in a similar way as the CRS applies to Financial Accounts.

11. The CARF therefore brings tax transparency to the Crypto-Asset sector which, once implemented, imposes obligations on a new subset of service providers, RCASPs, which are the service providers best positioned to collect and report information on transactions of Crypto-Assets. Specifically, the CARF requires RCASPs to identify their users and to report on specified transactions, with a view to ensuring the annualised reporting of tax relevant information concerning certain activities in relation to Crypto-Assets. Once received by tax authorities, the information will be automatically exchanged with the tax authorities of the jurisdiction(s) of residence of the Crypto-Asset Users, pursuant to an international agreements that provides a legal basis for the automatic exchange of information for tax purposes.

12. While the CARF is considered to be an "integral part" of the international standards for AEOI, which also includes the CRS, it is a standalone framework from the CRS and other forms of AEOI as it applies to the Crypto-Asset sector.[8] Nevertheless, the CARF shares several features with the CRS that are relevant for tax administrations and service providers to understand possible approaches to implementation. These similarities include the annualised reporting and exchange of information, the due diligence procedures to be followed, as well as the IT and confidentiality requirements. It is therefore useful, as a starting point, to review the similarities and differences between the CARF and the CRS. It should also be noted that the CARF helps strengthen the CRS by removing a route for the CRS to be circumvented.[9]

Table 1: CARF Compared to the CRS	
Similarities to the CRS	**Annualised reporting and exchange**: Like the CRS, the CARF applies annualised reporting requirements that support annual automatic exchanges between tax authorities. RCASPs collect and report the pre-defined information to tax authorities, which subsequently exchange the information with the tax administrations of partner jurisdictions pursuant to an international agreement that provides a legal basis for the automatic exchange of information for tax purposes. **Due diligence**: To the extent possible and appropriate, the CARF due diligence procedures are consistent with the CRS due diligence procedures, to minimise burdens on RCASPs when they are also subject to CRS obligations as Financial Institutions. The CARF also allows RCASPs that are subject to the CRS to rely on the due diligence procedures for New Accounts performed for CRS purposes. **IT systems**: Like the CRS, the CARF requires certain IT systems to be put in place by tax authorities and reporting service providers to ensure that RCASPs and jurisdictions can report and exchange the required information respectively. In many cases, existing systems used by tax authorities for CRS exchanges can likely be expanded to support CARF exchanges. **Confidentiality requirements**: Similarly to the CRS, the CARF requires jurisdictions to have appropriate confidentiality and data safeguards (CDS) in place and the requirements are essentially the same as for the CRS. In this regard, all jurisdictions that implement the CRS undergo CDS assessments by the Global Forum pre- and post-exchange. Given that these assessments cover the scope of issues that concern AEOI in general, the assessments can be expected to continue to be relied upon, to the extent that the analysis and conclusions are applicable to the CARF (which is generally expected to be the case).
Distinguishing the CARF from the CRS	**Scope of assets**: The CARF applies to a set of assets that differs from those covered by the CRS. While the CRS covers traditional money, securities, and other financial products (i.e. Financial Accounts), the CARF is concerned with Crypto-Assets. These assets are distinguishable from Financial Accounts as they rely on cryptography and distributed ledger technology, in particular blockchain technology, to be issued, recorded, transferred and stored. This is done in a decentralised manner,

[8] G20 Leaders' Declaration Bali, Indonesia, 15-16 November 2022.

[9] Furthermore, jurisdictions planning to implement the recent amendments to the CRS (published alongside the CARF) may decide to coordinate their domestic implementation of the CARF to ensure coherence in the reporting requirements for Entities simultaneously considered to be Financial Institutions under the CRS and Reporting Crypto-Asset Service Providers under the CARF.

without the need to rely on traditional financial intermediaries or central administrators.

Scope of reporting service providers: As opposed to the CRS, which covers Financial Institutions, the CARF covers a different set of reporting service providers, RCASPs, which are required to perform the due diligence and reporting (noting that some service providers might qualify both as Financial Institutions and RCASPs). RCASPs are defined in a functional manner to include both individuals and Entities that provide services effectuating Exchange Transactions in relevant Crypto-Assets. Hence, while Financial Institutions can be RCASPs, the definition of RCASP also includes actors that are not covered under the CRS. RCASPs that are not Financial Institutions may have no experience with tax information collection and reporting given that they have not been subject to CRS.

The information reported: While the CRS requires the annual reporting of account balances and information on payments and proceeds from sales of Financial Assets, the CARF has transaction-based reporting requirements of exchanges between Relevant Crypto-Assets and Fiat Currencies; exchanges between one or more forms of Relevant Crypto-Assets; and transfers of Relevant Crypto-Assets. These transactions will be reported with respect to a user on an aggregate basis by type of Relevant Crypto-Asset, distinguishing the type of transactions.

Reporting schema: Similarly to the CRS requiring the use of the dedicated CRS XML Schema and User Guide for the CRS exchanges between tax authorities, reflecting the differences in the scope of assets and reporting requirements, the CARF has a dedicated CARF XML Schema and User Guide for the CARF exchanges. Jurisdictions could also consider using the CARF XML Schema domestically for the purpose of gathering the required information from their respective RCASPs.

13. The remainder of this document has three Chapters: the first focuses on the legal frameworks that jurisdictions must put in place to implement the CARF, including to impose the due diligence and reporting obligations on RCASPs; the second focuses on the administrative and IT frameworks that need to be put in place by RCASPs and jurisdictions to implement the CARF; and the third describes the due diligence and reporting rules found in the CARF, to provide an initial high-level reference guide on the CARF rules.

1. The legal frameworks necessary to implement the CARF

14. This Chapter is intended to provide background information on the legal frameworks involved in the effective implementation of the CARF.

Enacting a legal framework for the CARF

15. Once a jurisdiction has made a political commitment to implement the CARF, its next step will be to implement the requirements of the CARF in its legal framework. Jurisdictions will need to reflect both domestic and international legal requirements in order to operationalise the CARF. The considerations and processes in this regard are similar to those faced when implementing the CRS.

Domestic legal requirements

16. In order to deliver a commitment to implement the CARF, a jurisdiction needs to translate the relevant definitions, due diligence and reporting obligations, and effective enforcement provisions, provided for in the CARF, into its domestic law. This will identify the RCASPs obliged to report information to the jurisdiction, establish the scope of the information that should be collected with respect to the RCASP's users, along with the prescribed due diligence requirements to identify such users and outline the information that RCASPs must report. Jurisdictions will also need legal frameworks to enable them to ensure compliance with the CARF and to enforce its requirements.

17. In order to ensure that the CARF is fully implemented, the domestic framework imposing the due diligence and reporting rules on RCASPs must be legally binding and must incorporate the required elements set out in the rules of the CARF. It should also be ensured that the rules of the CARF are interpreted in accordance with its commentary.

18. To ensure RCASPs fulfil their due diligence and reporting requirements on time, the latest date by which the domestic laws will have to be in place and take effect is from the start of the calendar year (or other appropriate reporting period) before the first year the jurisdiction commits to exchange information under the CARF. Notwithstanding that, it is important to provide RCASPs with clarity on the requirements of such domestic laws sufficiently in advance of this date for them to properly prepare (such as by putting in place the necessary systems and procedures to conduct the necessary due diligence on their users from the start of the reporting period).

19. These considerations and the applicable processes are similar to those that apply in relation to implementing the domestic legal requirements with respect to the CRS.

20. Chapter 3 provides a description and further details of the due diligence and reporting rules themselves.

International legal requirements

21. In addition to domestic legal requirements, to deliver a commitment to implement the CARF, jurisdictions will need to have in place an international legal framework that permits the automatic exchange of information under the CARF. Firstly, this requires an international legal basis that provides for the automatic exchange of information between jurisdictions. The Convention on Mutual Administrative Assistance in Tax Matters (MAAC), which CRS implementing jurisdictions use for automatic exchange under the CRS, can also be used to provide an international legal basis supporting CARF exchanges. Jurisdictions can also establish automatic exchange relationships based on bilateral double tax treaties or Tax Information Exchange Agreements that permit the automatic exchange of information. Regional approaches (such as in the European Union for EU Member States) can also be put in place.

22. Secondly, once a legal basis is in place, jurisdictions will need to put in place administrative agreements to determine the information to be exchanged and the time and method of the exchanges. As with the legal basis, these agreements can take various forms, such as multilateral or bilateral Competent Authority agreements, self-standing intergovernmental agreements or regional approaches.

23. The CARF Multilateral Competent Authority Agreement (MCAA) is included in the CARF package[10] and, similarly to the CRS MCAA, is based on the MAAC to provide for a multilateral means of putting in place administrative agreements to exchange CARF information. As with the CRS MCAA, while the CARF MCAA is a multilateral agreement, the individual bilateral exchange relationships are only created through a subsequent activation process. In this regard, a CARF exchange relationship pursuant to the CARF MCAA will only be activated with another jurisdiction if both jurisdictions have the MAAC in force and in effect and have lodged the required CARF MCAA notifications with the CB Secretariat and incorporated each other in their list of intended exchange partners (i.e. CARF MCAA notification pursuant to Section 7(1)(g)).

[10] International Standards for Automatic Exchange of Information in Tax Matters, 2023, page 69 et seq., https://www.oecd-ilibrary.org/taxation/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.

2. The administrative and IT frameworks necessary to operationalise the CARF

24. This Chapter is intended to provide background information on the administrative and IT frameworks involved in the effective implementation of the CARF. It contains considerations for both jurisdictions and RCASPs.

General considerations

25. In addition to a domestic and international legal framework requiring RCASPs to carry out the due diligence and reporting obligations and providing for the international exchange of the information, jurisdictions will need to have in place the relevant administrative framework, for which RCASPs will also need policies and procedures to comply with. Furthermore, both jurisdictions and RCASPs will need respective IT capabilities. Each of these elements will be required to ensure that the due diligence, reporting and exchange requirements of the CARF are effectively implemented in practice.

26. For many aspects of the administrative and IT requirements of the CARF, the procedures and systems that jurisdictions have already developed and implemented to support the CRS can be leveraged in the context of the CARF. This is particularly relevant for jurisdictions that have implemented the CRS and for RCASPs that are also Reporting Financial Institutions in the context of the CRS. Notwithstanding that, time will be needed to develop and put in place the administrative frameworks, associated policies and procedures, as well as the IT requirements that are needed to operationalise the CARF. This can be expected to require additional time and focus for jurisdictions that have not implemented the CRS and for RCASPs that are not also Reporting Financial Institutions under the CRS.

Administrative frameworks to ensure the effective implementation of the CARF

27. The effectiveness of the implementation of the CARF will depend upon RCASPs complying with the due diligence and reporting requirements. It will also depend upon tax administrations implementing proportionate, risk-based and comprehensive compliance and enforcement strategies to ensure RCASPs are meeting their reporting requirements and, in turn, exchanging information with other jurisdictions.

28. An effective administrative framework to ensure compliance will include jurisdictions proactively and collaboratively engaging with RCASPs so that they understand the due diligence and reporting requirements and the frameworks with which they will need to comply, along with the fact that authorities will verify compliance and enforce the requirements where they are found as not being met.

29. This will be particularly important in the context of the Crypto-Asset sector, as the service providers, such as Crypto-Asset exchanges, may currently only be subject to limited or no regulatory

oversight and reporting obligations and will therefore have limited experience of the types of requirements contained in the CARF and the consequences of not complying.

30. Similar to the CRS, a jurisdiction's CARF compliance strategy will need to be designed to ensure the effective implementation of the due diligence and reporting obligations, taking into account the jurisdiction's particular domestic legal, regulatory and administrative context. Firstly, this includes the identification of the Entities and individuals that, by virtue of their activities, are RCASPs and that have a nexus within the jurisdiction in order to ensure that they report information as required. Secondly, a jurisdiction's strategy will also need to ensure that RCASPs accurately follow the due diligence and reporting procedures of the CARF, including through raising awareness of, and promoting compliance with the CARF. Finally, a jurisdiction will need to verify and enforce compliance with, the CARF, including by having an appropriate penalty and enforcement framework to address instances of non-compliance. These high-level considerations are expanded on below.

Identifying RCASPs that have a nexus within a jurisdiction

Considerations for RCASPs

31. Once a jurisdiction implements the CARF, service providers will need to determine whether they are RCASPs that are subject to the associated due diligence and reporting requirements in that jurisdiction.

32. First, a service provider will need to determine whether it is a RCASP. Section IV B of the CARF, which should be reflected in the jurisdiction's domestic legal framework, defines a RCASP as "any individual or Entity that, as a business, provides a service effectuating Exchange Transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary, to such Exchange Transactions, or by making available a trading platform." The CARF sets out further details of the meanings of each of the relevant terms.

33. Second, a RCASP will need to determine the jurisdiction(s) to which it should report information under the CARF. The nexus criteria in Section I of the CARF, which should be reflected in an implementing jurisdiction's domestic legal framework, consider a RCASP as subject to the due diligence and reporting requirements in a jurisdiction if it is:

- an Entity or individual resident for tax purposes in the jurisdiction; or
- an Entity that (a) is incorporated or organised under the laws of the jurisdiction, and (b) either has legal personality in the jurisdiction or has an obligation to file tax returns or tax information returns to the tax authorities in the jurisdiction with respect to the income of the Entity; or
- an Entity managed from the jurisdiction; or
- an Entity or individual that has a regular place of business in the jurisdiction.

34. To avoid duplicative reporting where a RCASP has a nexus in more than one Partner Jurisdiction[11], Section I of the CARF sets out that the hierarchy amongst these nexus criteria is the order in which they are set out above. There is also a rule to address situations where a RCASP is subject to the same nexus in two or more Partner Jurisdictions. Additionally, Section I contains special rules to address situations where a RCASP effectuates Relevant Transactions through a Branch.

[11] The term "Partner Jurisdiction" means any jurisdiction that has put in place equivalent legal requirements and that is included in a list published by [Jurisdiction]. See, Section IV.F(1), International Standards for Automatic Exchange of Information in Tax Matters - Crypto-Asset Reporting Framework and 2023 updates to the Common Reporting Standard, 8 June 2023: https://www.oecd.org/tax/international-standards-for-automatic-exchange-of-information-in-tax-matters-896d79d1-en.htm.

35. RCASPs will need to understand the RCASP definition and the nexus rules of CARF, as implemented by jurisdictions, in order to determine in which jurisdiction(s) the RCASP has nexus to and therefore where it will need to report CARF information. In many cases, notably where a RCASP is tax resident or incorporated or organised in a jurisdiction, the primary nexus will be readily determinable. In other cases, a RCASP may only have a nexus by being managed from or having a regular place of business in a jurisdiction. The CARF requires fewer connections to a jurisdiction than the traditional standards for tax residence or permanent establishment in a jurisdiction, and consequently a RCASP may have CARF reporting obligations to a jurisdiction that it does not otherwise pay taxes to or report tax information to. A RCASP may also have nexus to multiple jurisdictions, in which case it must determine whether one nexus is more significant than others (according to the hierarchy set out in the CARF), or whether rules to address situations where a RCASP is subject to the same nexus in two or more Partner Jurisdictions may apply.

Considerations for jurisdictions

36. In addition to RCASPs correctly identifying themselves and the jurisdiction(s) to which they are required to report information, jurisdictions will need to verify that the requirements are being complied with to ensure compliance by RCASPs.

37. In certain circumstances, jurisdictions may be able to largely rely on domestic regulatory frameworks already in place for other purposes (e.g. AML or financial markets registration requirements) to identify RCASPs if the framework generally corresponds with the scope of the CARF. For example, jurisdictions may rely in part on a domestic regulatory framework in place for purposes of the requirements of FATF's Recommendation 15. However, such frameworks would not be sufficient to ensure that all RCASPs are identified, for several reasons. First, the definition of RCASP is broader than the FATF's definition of a Virtual Asset Service Provider (VASP).[12] One way in which it is broader is that the CARF has a broader definition of Relevant Crypto-Assets than the FATF definition of Virtual Assets, and a NFT that is not a Virtual Asset for FATF may be a Relevant Crypto-Asset for CARF. Accordingly, platforms for exchanging NFTs may not be VASPs, but they could be RCASPs. Second, the nexus rules in the CARF are much broader than the corresponding requirements in the FATF Recommendation. Therefore, a domestic regulatory framework may be helpful in identifying RCASPs, but a jurisdiction will need additional mechanisms in its administrative framework in order to fully implement the CARF.

38. Such additional mechanisms should take into account that RCASPs may be organised in different ways (as described above), so new techniques may be necessary, for example, to identify RCASPs that provide services without the use of a legal entity but that are managed from the jurisdiction. This could be because key personnel are based in the jurisdiction, or there is a regular place of business in the jurisdiction, such as a customer support centre based in the jurisdiction. There may even be no single jurisdiction where the core functions are carried out, in light of the entirely online nature of Crypto-Asset services. The criteria of "managed from the jurisdiction" and "regular place of business" are therefore intended to be broader criteria than the jurisdiction where effective management takes place or where a principal place of business is located.

39. If a jurisdiction determines that its existing domestic regulatory framework would not ensure the identification of certain or all RCASPs with a nexus to its jurisdiction, it will need to put in place additional mechanisms to ensure RCASPs with a nexus to its jurisdiction are identified. Examples of possible solutions to identify RCASPs are provided in the Commentary to Section V of the CARF. They include a requirement for RCASPs to proactively register with a domestic centralised registry, which could be

[12] For purposes of this document, reference should be made to the definition of VASP found in the November 2023 version of the FATF Recommendations. See, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

complemented by a nil reporting requirement, mechanisms (e.g. an anonymous tip line or inbox) whereby information about non-compliant RCASPs could be reported to the authorities and the introduction of a requirement on domestic Crypto-Asset Users to report, for instance in their tax returns, the name and address of the RCASPs that they have used.

40. In addition to the options set out above, a possible mechanism jurisdictions may consider to identify RCASPs and whether they should be reporting information to the jurisdiction could be one built on the notification foreseen in Section I.H of the CARF, which requires a RCASP to lodge a notification with a jurisdiction where it has a nexus, if it has completed its due diligence and reporting requirements in another jurisdiction where it has a substantially similar nexus. Given the utility of the information that would be reported under such a mechanism, jurisdictions may consider expanding this provision in their domestic implementation of the CARF to also require the filing of such a notification in situations where a RCASP has reported in another jurisdiction also implementing the CARF because it has a *higher* nexus in that jurisdiction, as set out under Section I.A of the CARF. This could be used to identify RCASPs that have a nexus in the jurisdiction, as well as to obtain assurance that a RCASP is not expected to report information in the jurisdiction because the RCASP is already fulfilling the requirements of the CARF and reporting the relevant information in another jurisdiction.

41. Ultimately, each jurisdiction may choose the exact administrative approach(es) it uses to identify RCASPs with due diligence and reporting requirements in its jurisdiction. That choice will involve many considerations, however, regardless of the approach(es) taken, it needs to be sufficiently robust so as to achieve the objective of identifying RCASPs with a nexus in the jurisdiction.

Ensuring RCASPs fulfil the due diligence and reporting requirements

Considerations for RCASPs

42. Once the CARF is implemented by a jurisdiction, RCASPs that need to report information to that jurisdiction will be required to accurately follow the due diligence and reporting procedures contained in the CARF. This will require the RCASPs to understand the due diligence and reporting requirements and to put in place the administrative and IT requirements to ensure they are followed. Chapter 3 provides a high-level description and further details of the due diligence and reporting rules themselves.

Considerations for jurisdictions

43. Jurisdictions will need to gain assurance that RCASPs are correctly implementing the due diligence and reporting rules, including through actions to verify on the basis of a proportionate, risk-based and comprehensive compliance strategy and to enforce the requirements as necessary.

44. This will require jurisdictions to designate appropriate administrative bodies (e.g. a tax authority or financial supervisor) and to ensure they have the necessary powers to verify the compliance of RCASPs with the due diligence and reporting obligations and to enforce the requirements as necessary. These powers will need to include imposing adequate administrative and/or criminal penalties on RCASPs for failure to comply with the due diligence and reporting procedures described in Sections II and III of the CARF, as well as to keep records. This includes having in place strong measures to ensure valid self-certifications are always collected. Jurisdictions will also need to devote adequate resources to properly verify and enforce the compliance of RCASPs with the due diligence and reporting requirements.

45. The designated authorities should then develop and implement suitable policies and procedures, including activities to verify compliance with the requirements and to deter and address instances of noncompliance.

Raising awareness of the CARF

46. As previously mentioned, RCASPs will need to understand the due diligence and reporting obligations of the jurisdiction to which they are required to report. It is also important they are aware of the administrative actions, penalties and other sanctions potentially applicable in cases of non-compliance.

47. Some RCASPs (e.g. Financial Institutions) are likely to be well-established actors in the traditional financial sector and are therefore likely aware of relevant regulatory and reporting requirements. However, many other RCASPs may be emerging actors less aware of such requirements. Therefore, to establish effective compliance and enforcement frameworks, jurisdictions should ensure that the CARF requirements are widely disseminated and publicised, especially during the initial years of CARF implementation. The objective is to ensure that, by the time their collection and reporting obligations become effective, RCASPs will have received the information they need to comply with the due diligence and reporting obligations of the CARF.

48. Such awareness raising might include jurisdictions communicating with the RCASP sector through available channels, such as through published guidance or FAQs that set out a jurisdiction's implementation of the CARF in an accessible manner, and/or the provision of other supporting materials. Based on the number and types of RCASPs present, a jurisdiction could decide whether to provide sector specific guidance, in addition to more generalised materials. Jurisdictions could also consider establishing a helpline or dedicated email address to respond to specific queries. As above, the ways in which jurisdictions disseminate guidance on the CARF will vary, but the goal of educating RCASPs on their collection and reporting obligations is shared among all jurisdictions implementing the CARF.

49. Finally, depending on the jurisdiction, it may be relevant to consider that at least some RCASPs may be emerging actors currently subject only to limited or no regulation and therefore may not yet be identified by regulatory authorities. Where some RCASPs with a nexus in a jurisdiction might not be easily identifiable and may potentially not be aware of their due diligence and reporting obligations, jurisdictions may make additional efforts to conduct outreach to such RCASPs as needed, such as by hosting webinar sessions where the requirements of the domestic legislation and necessary compliance activities could be explained in further detail. Government officials may also consider participating in conferences or other industry events to further raise awareness.

Ensuring the effective implementation of the CARF in practice

50. In addition to raising awareness of the CARF in order to facilitate RCASPs in fulfilling their obligations, jurisdictions should implement sufficiently robust administrative compliance and enforcement strategies that include activities to verify that RCASPs are effectively implementing the requirements in practice. As set out above, such activities can be broadly considered to involve two elements: firstly, ensuring that all RCASPs are reporting as required; and, secondly, ensuring that the information they report is in line with the due diligence and reporting rules in the CARF.

51. With respect to ensuring that all RCASPs are reporting as required, once a jurisdiction has identified the service providers that are potentially required to report information (see above), a basic activity jurisdiction should take is to compare that group to service providers that actually did report information, to account for any discrepancies. Jurisdictions should investigate such discrepancies in line with their compliance strategies. With respect to ensuring that the information being reported is complete and accurate actions can include analysing the information reported to identify possible errors or non-compliance and in-depth audits to review the documentation held by RCASPs. Where issues are found, enforcement action should be considered as appropriate, with a view to correcting and deterring non-compliance.

The IT frameworks for the reporting and exchange of the CARF information

The domestic reporting of the information

52. Once implemented in a jurisdiction, the CARF includes an obligation on the RCASPs in that jurisdiction to conduct the due diligence rules and report the required information in the implementing jurisdiction (subject to the nexus rules above). In order for RCASPs to comply with this obligation, implementing jurisdictions will need to put in place mechanisms to allow for this reporting in a manner appropriate for its legal and administrative context.

Considerations for RCASPs

53. RCASPs in an implementing jurisdiction will need to establish procedures and build systems in order to collect and report CARF information to the relevant authority. The systems will need to be capable of ensuring the collection of information in accordance with the CARF in order for it to be reported to the jurisdiction. RCASPs will also need to familiarise themselves with the mechanisms and requirements put in place by the implementing jurisdiction for the reporting of the information in order to ensure that the information can be successfully reported. In this regard, jurisdictions will be seeking to ensure that the contents of the information reported is consistent with the requirements of the CARF XML Schema (e.g. that the reported information includes the necessary data to be in compliance with the validation fields in the CARF XML Schema). Where applicable (i.e. where RCASPs are also Financial Institutions for the purposes of the CRS), the procedures and systems developed in relation to the CRS may be further built upon by RCASPs to implement the CARF.

Considerations for jurisdictions

54. Once the jurisdiction receives information from its RCASPs, it will need to prepare the information so that it can be exchanged in a manner that meets the requirements of the CARF (i.e. is consistent with the dedicated CARF XML Schema and User Guide), through exchange mechanisms that maintain the integrity and security of the information.

55. With respect to the domestic reporting requirements, given the similarities in the technical requirements between the CRS and the CARF, jurisdictions that have already implemented the CRS may be able to expand those systems to support domestic reporting by RCASPs under the CARF. Other jurisdictions may need to build new systems to implement the CARF. Whatever the technical solution, it should include validations to ensure that the data reported is consistent with the requirements, so that the files for exchange can be prepared in line with the CARF XML Schema and User Guide. Failing to validate the information upfront will likely result in further follow-up being required by jurisdictions with RCASPs for the jurisdiction to meet the requirements before the jurisdiction is able to send the information to its partners in a manner that is consistent with the CARF XML Schema and User Guide.

56. While it is not a requirement, jurisdictions may also use the CARF XML Schema and User Guide (or compatible domestic versions of the Schema) for the domestic reporting of information by RCASPs.

The international exchange of the information between tax authorities

57. Once the information has been prepared by the jurisdiction consistent with the CARF XML Schema and User Guide, it needs to be exchanged with the jurisdiction’s exchange partners in a secure and encrypted manner, as required by the CARF.

58. While other transmission methods may be used, the Global Forum manages the provision of the Common Transmission System (CTS) for jurisdictions to exchange tax information amongst each other, on a bilateral basis. It is used by all jurisdictions exchanging information under the CRS. Jurisdictions

currently using the CTS will also be able to use the CTS for exchanging information under the CARF. Jurisdictions not currently using the CTS will be able to onboard onto the CTS for CARF exchanges.

59. Jurisdictions can exchange information using the CTS either through manual methods (i.e. the push-pull method) or through system-to-system exchanges (SFTP). As with the CRS, jurisdictions can therefore develop such systems to link with the CTS to carry out the exchanges with respect to the CARF.

Specific considerations for jurisdictions in the first year of implementation

60. As indicated previously, the first group of jurisdictions to exchange information under the CARF is expected to commence exchanges in 2027 or, at the latest, 2028.

61. Given that the CARF is a new reporting framework and will apply to many service providers that are likely to be unfamiliar with tax reporting, jurisdictions are encouraged to place due focus in the first years of the CARF's implementation on raising awareness of the CARF and the potential reporting obligations of RCASPs that may have a nexus within its jurisdiction, and on educating RCASPs on their compliance obligations. Also, jurisdictions are encouraged to take into account, within the limits of the applicable national provisions, whether RCASPs have made reasonable efforts to comply with the requirements of the CARF in considering the application of domestic penalty or enforcement regimes and to allow RCASPs that have made compliance errors time to correct their mistakes.

62. Furthermore, during this initial period of implementation, it is possible that a RCASP could have its reporting nexus to a jurisdiction that is commencing exchanges in 2027, but then in the following year be required to report to a jurisdiction that is commencing exchanges in 2028 (i.e. because the RCASP has a higher nexus to the 2028 jurisdiction, according to the hierarchy of the CARF nexus rules). Because it is not ordinarily the case that a reporting intermediary is required to report to tax authorities in two different jurisdictions from one year to the next, absent a change in its legal organisation, place of effective management or operational activities, these nexus rules could lead a RCASP to be subject to differing frameworks in the first years of CARF implementation, thereby imposing additional costs on RCASPs in order to comply. Therefore, in order to facilitate the smooth transition to the CARF, minimise the additional costs imposed on such RCASPs from having to move their reporting between jurisdictions, and to minimise the risk of issues that could undermine the effectiveness of the CARF, it is recommended that - unless it would incur unreasonable administrative costs for jurisdictions - such RCASPs be able to report information in 2027 in accordance with the dedicated CARF XML Schema and User Guide, without modification, such as of the data fields.[13] This is because any jurisdiction-specific modifications would only be used by such a RCASP for 2027 reporting, after which they would move their reporting to the jurisdiction with a highest nexus. The use of bespoke schemas or data fields in such cases would therefore impose unnecessary additional costs.

---

[13] OECD (2024), *Crypto-Asset Reporting Framework XML Schema: User Guide for Tax Administrations*, OECD Publishing, Paris, https://doi.org/10.1787/578052ec-en.

3. Overview of the due diligence and reporting rules of the Crypto-Asset Reporting Framework

63. This Chapter provides an overview of the CARF and summarises the due diligence and reporting rules therein. It is intended to provide an initial high-level reference guide to the requirements that RCASPs need to comply with to implement the CARF.

An overview of the Crypto-Asset Reporting Framework

64. The central part of the CARF are the definitions, detailed rules and procedures that RCASPs must follow in order to ensure the relevant information is collected and reported. These are the rules that must be incorporated into domestic law to ensure that RCASPs perform the due diligence and reporting requirements correctly and can be broken down into a series of separate steps. Each of these steps is discussed in-depth throughout this chapter.

Section 1: Reporting Crypto-Asset Service Providers

Definition of Reporting Crypto-Asset Service Providers

65. To ensure the successful implementation of the CARF, an initial key consideration is ensuring the correct service providers are required to collect and report information to tax administrations in the correct jurisdictions. The CARF defines RCASPs as an Entity or individual that, as a business, provides a service

effectuating Exchange Transactions for or on behalf of customers.[14] The CARF establishes reporting requirements on RCASPs in the jurisdictions where they have sufficient connections (i.e. a nexus). These definitions therefore require considering the following steps when determining whether a service provider is a RCASP.

An Entity or individual …

66. The first step is to determine whether an Entity or individual is acting as a RCASP. Note that, as opposed to the CRS, which specifies that only Entities can be Reporting Financial Institutions, the CARF specifies that RCASPs can be either Entities or individuals. Similarly to the CRS, the term "Entity" covers a wide range of legal persons and legal arrangements other than an individual (i.e. a natural person).[15] Thus, for example, a corporation, partnership, trust, fideicomiso, foundation (fondation, Stiftung), company, co-operative, association, or asociación en participación, falls within the meaning of the term "Entity".

67. Individuals are also included in the definition of RCASP, given that the services of RCASPs can be offered equally by individuals as by Entities. Hence, an individual meeting the requirements of the definition would be considered a RCASP. In addition, a group of individuals meeting the requirements of the definition would be considered a RCASP or multiple RCASPs. Specifically, an individual or Entity that as a business, provides a service effectuating Exchange Transactions for or on behalf of customers, including by making available a trading platform, is a RCASP. The technology involved in providing such service is irrelevant to determine whether an individual or Entity is a RCASP. An individual or Entity will be considered to make available a trading platform to the extent it exercises control or sufficient influence over the platform, allowing it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform. This may occur through the coordinated efforts of multiple individuals and/or Entities, which may be located in multiple jurisdictions. In such cases, each individual or Entity that exercises control or sufficient influence over the platform is considered an RCASP.[17] For such scenarios, the CARF due diligence rules provide for the option of RCASPs to designate a single party to fulfil the due diligence requirements of the RCASP.

… that provides a service effectuating Exchange Transactions …

68. The RCASP definition is functional and based on the set of activities such service providers engage in. Specifically, a RCASP must effectuate Exchange Transactions on behalf of customers. "Effectuating Exchange Transactions" refers to a service through which the customer can receive Relevant Crypto-Assets for Fiat Currencies, or vice versa, or exchange Relevant Crypto-Assets for other Relevant Crypto-Assets. The CARF identifies a number of different types of activities that, when performed as a business, are to be considered effectuating Exchange Transactions and therefore giving rise to classification as a RCASP. A RCASP may effectuate transactions in Crypto-Assets in a manner similar to a traditional financial institution, by acting as a dealer or broker with respect to those assets, or it may effectuate transactions in Crypto-Assets by providing access to "decentralised" services such as software that automatically matches a buyer and seller and facilitates Exchange Transactions between those Crypto-Asset Users. Additional relevant terminology, as defined in the CARF, is provided below.

Explanation of Relevant Terminology -- Crypto-Assets

[14] International Standards for Automatic Exchange of Information in Tax Matters, 2023, CARF - Section IV.B(1) and Commentary thereto, pp. 22 and 53-54: https://www.oecd-ilibrary.org/taxation/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.

[15] International Standards for Automatic Exchange of Information in Tax Matters, 2023, CARF - Section IV.F(3) and Commentary thereto, pp. 27 and 62: https://www.oecd-ilibrary.org/taxation/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.

The term “Crypto-Asset” refers to a digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions. A “digital representation of value” means that a Crypto-Asset must represent a right to value, and that the ownership of, or right to, such value can be traded or transferred to other individuals or Entities in a digital manner. The definition of Crypto-Asset is thus functional and does not depend on labels that may be used to describe it, such as “cryptocurrency,” “security token,” or “non-fungible token,” all of which may be Crypto-Assets.

For further information, see CARF, Section IV.A(1) and Commentary thereto.

Explanation of Relevant Terminology -- Relevant Crypto-Assets

While the definition of Crypto-Assets is intended to cover a broad range of assets, not all Crypto-Assets are subject to the scope of the CARF. Relevant Crypto-Assets are Crypto-Assets in respect of which RCASPs must fulfil reporting and due diligence requirements. If an individual or Entity is a RCASP (e.g. because it otherwise carries out exchanges in Relevant Crypto-Assets), it would nevertheless not be required to report information with respect to exchanges carried out in Crypto-Assets that are not Relevant Crypto-Assets.

The term Relevant Crypto-Assets applies to all Crypto-Assets except three types:

- Central Bank Digital Currencies,
- Specified Electronic Money Products, and
- Crypto-Assets for which the RCASP has adequately determined that they cannot be used for payment or investment purposes. Other Crypto-Assets (other than the two types listed above) are treated as usable for payment or investment purposes unless a RCASP makes affirmative determination that they cannot be so used.

A Crypto-Asset that is treated as a Virtual Asset under FATF rules is considered a Relevant Crypto-Asset. Non-fungible tokens that are traded on a marketplace are treated as assets that can be used for payment or investment purposes and therefore would be considered Relevant Crypto-Assets. For further information, see CARF, Section IV.A(2) and Commentary thereto.

Explanation of Relevant Terminology -- Distributed Ledger Technology and Similar Technology

A Crypto-Asset must rely on a cryptographically secured distributed ledger or similar technology to validate and secure transactions. A distributed ledger is a decentralised manner for recording transactions in Crypto-Assets in multiple places and at the same time. Cryptography refers to a mathematical and computational practice of encoding and decoding data that is used to validate and secure transactions in a decentralised or non-intermediated manner. Validation refers to the process of confirming and recording a transfer or other transaction, similar to the settlement of a financial asset transaction. Crypto-Assets may also rely on similar technology that allows for the disintermediated holding or validating of Crypto-Assets.

For further information, see CARF, Commentary to Section IV.A(1).

Explanation of Relevant Terminology -- Fiat Currency
The term Fiat Currency refers to the official currency of a jurisdiction, issued by a jurisdiction or by a jurisdiction's designated Central Bank or monetary authority, as represented by physical banknotes or coins or by money in different digital forms, including bank reserves, and Central Bank Digital Currencies. For further information, see CARF, Commentary to Section IV.C(5).

Explanation of Relevant Terminology -- Central Bank Digital Currencies
The term "Central Bank Digital Currencies" means any digital Fiat Currency issued by a Central Bank. Central Bank Digital Currencies are not considered Relevant Crypto-Assets, given that they are a digital form of Fiat Currency. For further information, see CARF, Commentary to Section IV.A(3).

… on behalf of customers

Furthermore, an individual or Entity effectuating Exchange Transactions will only be a RCASP if it carries out such activities for or on behalf of customers. Hence, the simple passive investment of an investment fund investing in Relevant Crypto-Assets does not constitute a service effectuating Exchange Transactions since such activities do not permit the fund or its investors to effectuate Exchange Transactions. Furthermore, an individual or Entity that is solely engaged in validating distributed ledger transactions in Relevant Crypto-Assets, even if it receives payment for such purposes, is not considered to conduct Exchange Transactions on behalf of customers and, therefore, is not a RCASP.

Examples of RCASPs

Activities effectuating Exchange Transactions	Further explanation	Citation
Crypto-Asset exchanges that act as market makers and take a bid-ask spread as a transaction commission for their services.	This could include exchange services that provide liquidity to the Crypto-Asset market by bringing together orders for buyers and sellers.	CARF, Commentary to Section IV.B(1), page 53, paragraph 25.
Making available a trading platform that provides the ability for such customers to effectuate Exchange Transactions on such platform.	An individual or Entity is considered to make available a trading platform to the extent it exercises control or sufficient influence over the platform, that allows it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform. Individuals or Entities with control or sufficient influence over such a trading platform may be acting as RCASPs.	CARF, Commentary to Section IV.B(1), page 54, paragraph 26.
Operators of Crypto-Asset ATMs, permitting the exchange of Relevant Crypto-Assets for Fiat Currencies or other	Entities or individuals may also provide services effectuating Exchange Transactions where they run kiosks, such	CARF, Commentary to Section IV.B(1), page 53, paragraph 25.

Relevant Crypto-Assets through such ATMs.	as automated teller machines, that actively convert Relevant Crypto-Assets to Fiat Currencies or other Relevant Crypto-Assets via physical electronic terminals.	
Individuals or Entities subscribing one or more Relevant Crypto-Assets, such as the direct purchase of Relevant Crypto-Assets from an issuer, to resell and distribute such Relevant Crypto-Assets to customers.	Services provided as a market maker, subscriber or other market facilitator to acquire and/or dispose of Relevant Crypto-Assets would constitute effectuating an Exchange Transaction for purposes of the definition of RCASP. However, this would not include the sole creation and issuance of a Relevant Crypto-Asset.	CARF, Commentary to Section IV.B(1), page 54, paragraph 25.
Dealers acting for their own account to buy and sell Relevant Crypto-Assets to customers.	This can include individuals or Entities who stand ready to, as part of its regular business, to buy or sell Relevant Crypto-Assets with other customers, while acting as a principal for their own account.	CARF, Commentary to Section IV.B(1), page 53, paragraph 25.
Brokers in Relevant Crypto-Assets where they act on behalf of clients to complete orders to buy or sell an interest in Relevant Crypto-Assets.	As for other brokerage services in relation to traditional Financial Assets, this can cover the actions of brokers to exchange Relevant Crypto-Assets with other Relevant Crypto-Assets and/or Fiat Currencies on behalf of their customers in an agent or intermediary capacity.	CARF, Commentary to Section IV.B(1), page 53, paragraph 25.

Conducting activities “as a business’”

69. When effectuating Exchange Transactions on behalf of customers, a RCASP must be carrying on the activities “as a business”. The phrase “as a business” is meant to ensure the CARF does not place reporting requirements on individuals or Entities who effectuate Exchange Transactions but do not do so as part of a business (e.g. on a very infrequent basis for non-commercial reasons). In this regard, one-off transactions that are completed on behalf of other persons do not constitute conducting activities “as a business”. To determine the specific situations intended to be considered providing services “as a business”, implementing jurisdictions should reference their relevant domestic rules of interpretation.

Identifying where RCASPs should report

70. Once a RCASP has been correctly identified, the next step is to ensure that it has sufficient connections to a jurisdiction implementing the CARF, such that it can be effectively compelled by domestic authorities to report the required information to such jurisdiction’s tax authority. RCASPs with sufficient connections to an implementing jurisdiction are considered to have a reporting nexus to that implementing jurisdiction.

71. Section I of the CARF sets out the criteria pursuant to which a RCASP will be considered to have a nexus in a given jurisdiction. Furthermore, it is recognised that some RCASPs may have a nexus in more than one jurisdiction. The CARF therefore contains a hierarchy of nexus rules, with the intention that, where there are multiple jurisdictions where a nexus exists, the jurisdiction with the strongest link should be considered the primary jurisdiction for reporting purposes (i.e. a nexus higher on the list represents a

stronger link than a nexus lower on the list). For example, an Entity RCASP may have a nexus with two implementing jurisdictions of the CARF, where its tax residence is in one jurisdiction, while its place of incorporation is in a different jurisdiction. To prevent RCASPs from being subject to duplicate reporting requirements in multiple jurisdictions under such circumstances, a cascading hierarchy of nexus criteria requires the RCASP to report where it has the strongest link (in this case, in the jurisdiction of tax residence). If a RCASP has a nexus of the same priority (for example, a place of management) in two jurisdictions that have both implemented the CARF and have entered into an agreement to exchange CARF information, the RCASP can report in either jurisdiction, provided it lodges a notification in the jurisdiction where it does not report.

72. The reporting by Branches of RCASPs is also described under Section I of the CARF. A Branch means a unit, business or office of a RCASP treated as a branch for regulatory purposes. The general rule is that a RCASP is considered to have a regular place of business in any jurisdiction where it has a Branch. If the RCASP has a nexus that is higher in the hierarchy in another implementing jurisdiction, then the RCASP must generally comply with reporting and due diligence requirements in that other jurisdiction with respect to the Branch's activities, in addition to the jurisdiction where the Branch is located. However, the RCASP is relieved of those requirements with respect to the Branch's activities if the Branch itself reports the information to the tax authorities of the implementing jurisdiction in which it is located and such jurisdiction has an exchange agreement in place with the first jurisdiction. A RCASP that maintains one or more Branches fulfils the due diligence and reporting requirements with respect to a Crypto-Asset User if any one of its Branches in an implementing jurisdiction fulfils such requirements. This hierarchy of nexus rules is set out below.

Possible jurisdictions of nexus for RCASPs (CARF, Section I and Commentary thereto)	
Jurisdiction of tax residence	Refers to the jurisdiction where the RCASP (either an Entity or individual) has its tax residence. *Where should the RCASP report?* If an Entity RCASP reports in its jurisdiction of tax residence, then it has no reporting requirements in Partner Jurisdictions that are places of incorporation, management or regular place of business. Furthermore, an Entity RCASP is not required to complete reporting and due diligence requirements with respect to Relevant Transactions it effectuates through a Branch located in a Partner Jurisdiction, if the Branch itself completes the CARF reporting and due diligence requirements for these transactions in the Partner Jurisdiction. If an individual that is a RCASP reports in its jurisdiction of tax residence, then it has no reporting requirements in Partner Jurisdiction(s) where it has a regular place of business.
Jurisdiction of incorporation or organisation, where the Entity has legal personality or the obligation to files taxes	For Entity RCASPs, this criterion captures situations where an Entity RCASP (noting the wide definition of the term "Entity" in this context) is (a) incorporated or organised under the laws of a certain jurisdiction; and (b) subject to an obligation to file tax returns or tax information returns to the tax authorities in the jurisdiction with respect to its income.

	Where should the RCASP report? If an Entity RCASP reports in its jurisdiction of incorporation, then it has no reporting requirements in the Partner Jurisdictions where it has a place of management or regular place of business. Furthermore, an Entity RCASP is not required to complete reporting and due diligence requirements with respect to Relevant Transactions it effectuates through a Branch located in a Partner Jurisdiction, if the Branch itself completes the CARF reporting and due diligence requirements for these transactions in the Partner Jurisdiction.
Jurisdiction of management	For Entity RCASPs, this criterion captures the place of effective management, as well as any other place of management of the Entity. This criterion also includes situations where a trust (or a functionally similar Entity) that is a RCASP is managed by a trustee (or functionally similar representative) that is tax resident in a jurisdiction. *Where should the RCASP report?* If an Entity RCASP reports in its jurisdiction of management then it has no reporting requirements in Partner Jurisdiction(s) where there is a regular place of business. Furthermore, an Entity RCASP is not required to complete reporting and due diligence requirements with respect to Relevant Transactions it effectuates through a Branch located in a Partner Jurisdiction, if the Branch itself completes the CARF reporting and due diligence requirements for these transactions in the Partner Jurisdiction.
Jurisdiction that is a regular place of business	For Entity or individual RCASPs, this criterion captures a principal place of business, as well as other regular places of business of the RCASP. A Branch of an Entity RCASP is to be considered a regular place of business of such Entity RCASP. However, an Entity RCASP is not required to complete reporting and due diligence requirements with respect to Relevant Transactions it effectuates through a Branch located in a Partner Jurisdiction, if the Branch itself completes the CARF reporting and due diligence requirements for these transactions in the Partner Jurisdiction (see paragraph 49, above, for more details).

Section 2: Review Crypto-Asset Users to identify Reportable Persons, which include Crypto Asset Users and Controlling Persons of certain Entity Crypto Asset Users

73. Each RCASP needs to identify all Crypto-Asset Users and Reportable Persons with respect to which it must report information. Reportable Persons include Crypto-Asset Users that are Reportable Users (which may be individuals and Entities resident in a Reportable Jurisdiction) and Controlling Persons of certain Entity Crypto-Asset Users (essentially Entities that are not Active or otherwise excluded) that are resident in a Reportable Jurisdiction. Once RCASPs have identified all relevant Crypto-Asset Users and Reportable Persons, they need to determine whether any of the Relevant Transactions carried out on their

behalf should be reported to the tax authorities in accordance with the reporting requirements of Section II of the CARF. A Relevant Transaction means an Exchange Transaction or a Transfer of Relevant Crypto-Assets.

74. RCASPs must therefore first review and identify their customer base to determine whether any of their Crypto-Asset Users or the Controlling Persons of their relevant Entity Crypto Asset Users are subject to exclusions and should therefore not be reported on or are resident in a Reportable Jurisdiction (i.e. a jurisdiction with which the RCASP's jurisdiction has an exchange agreement). To make this determination, RCASPs will need to collect valid self-certifications for their Crypto-Asset Users and from the Controlling Persons of certain Entity Crypto-Asset Users. The relevant procedures are described in further detail below.

75. Unlike the CRS, the CARF due diligence rules apply substantive requirements equivalent to the CRS New Account Procedures for *both* Preexisting Crypto-Asset Users, as well as New Crypto-Asset Users (whether individuals or Entities, as well as the Controlling Persons of certain Entities). Indeed, the only difference between the due diligence requirements for Preexisting and New Crypto-Asset Users is one of timing: with respect to all Preexisting Crypto-Asset Users and the Controlling Persons of certain Entity Crypto-Asset Users (i.e. those with an existing relationship with the RCASP before the domestic effective date of the CARF rules), the RCASPs should carry out due diligence procedures equivalent to New Account Procedures with respect to all individuals or Entities identified as Crypto-Asset Users and the Controlling Persons of certain Entity Crypto-Asset Users, within 12 months of the effective date of such rules. With respect to New Crypto-Asset Users and the Controlling Persons of certain Entity Crypto-Asset Users, the RCASP is required to conduct due diligence and obtain a valid self-certification at the time of account opening, as well as one-off transactions.

76. Certain RCASPs may also be Financial Institutions under the CRS and already be required to conduct due diligence and reporting requirements under that framework in relation to their Account Holders. Recognising the need to avoid excessive duplication given that many Account Holders under the CRS may also be Crypto-Asset Users, the CARF due diligence rules provide that where a Financial Institution that is also a RCASP carries out due diligence procedures for new accounts under the CRS, such due diligence can also be relied on for purposes of fulfilling due diligence requirements under the CARF. Further, for purposes of completing the self-certification, the RCASP may rely on a valid self-certification collected in respect of the Crypto-Asset Users (whether Entities or individuals) or Controlling Person under the CRS or a valid self-certification already collected for other tax purposes, such as for domestic reporting purposes, in the context of the Foreign Account Tax Compliance Act (FATCA), or for purposes of a FATCA Intergovernmental Agreement, to the extent such self-certification contains all of the information required under the CARF.

Crypto-Asset Users

77. The first step is for RCASPs to identify their Crypto-Asset Users. The CARF specifies that a Crypto-Asset User is any individual (i.e. Individual Crypto-Asset User) or Entity (i.e. Entity Crypto-Asset User) for whom a RCASP carries out Relevant Transactions. Hence, any Individual Crypto-Asset Users as well as Entity Crypto-Asset Users must be identified by the RCASP.

78. In addition to identifying Crypto-Asset Users according to the general rule described above, there are also two distinct cases where RCASPs will need to apply specific rules for identifying Crypto-Asset Users.

- First, where a Crypto-Asset User (other than a RCASP or a Financial Institution) is acting for the benefit or account of another individual or Entity as an agent, custodian, nominee, signatory, investment advisor, or intermediary, the RCASP should not treat the intermediary as a Crypto-Asset User. Instead, the individual or Entity on whose behalf the Crypto-Asset User relationship is in place should be treated as the Crypto-Asset User, and identification should be carried out on that basis.

- Secondly, a RCASP may conduct Relevant Transactions (in this case, Transfers) that allow a merchant to offer its customers payment in the form of Relevant Crypto-Assets, in consideration of a purchase of goods or services, where the value exceeds USD 50 000. Depending on the RCASP's relationship with the merchant and the customer, either the merchant or the customer may be a Crypto-Asset User for the RCASP. In addition, if in the relationship only the merchant is the Crypto-Asset User with respect to the RCASP, but the RCASP is required to verify the identity of the merchant's customers pursuant to domestic anti-money laundering rules, the RCASP must then also treat the customers of the merchant as its Crypto-Asset User(s) and ensure their identification as such.

Using valid self-certifications to identify Crypto-Asset Users that are Reportable Users

79. Similar to the CRS, once the RCASP has identified its Crypto-Asset Users according to the above rules, it is required to identify whether any of its Crypto-Asset Users are Reportable Users and, on that basis, whether information in relation to those customers must be reported to the relevant tax authority, in line with the requirements of Section II of the CARF. RCASPs will make this determination on the basis of information obtained via the collection of valid self-certifications, as well as other information in their possession and, in certain cases, information that is publicly available. Overall, the process for identifying Crypto-Asset Users that are Reportable Users is very similar to requirements under the CRS.

Explanation of relevant terminology - Reportable Users and Reportable Persons

The term "Reportable User" means a Crypto-Asset User that is a Reportable Person.

The term "Reportable Person" means a Reportable Jurisdiction Person other than an Excluded Person.

For further details, see CARF Section IV.D(1) and (7), respectively, as well as the Commentary thereto.

Explanation of relevant terminology - Reportable Jurisdiction Person

The term "Reportable Jurisdiction Person" means an Entity or individual that is resident in a Reportable Jurisdiction under the tax laws of such jurisdiction, or an estate of a decedent that was a resident of a Reportable Jurisdiction. For this purpose, an Entity such as a partnership, limited liability partnership or similar legal arrangement that has no residence for tax purposes shall be treated as resident in the jurisdiction in which its place of effective management is situated. If the Entity Crypto-Asset User certifies that it has no residence for tax purposes, the RCASP may rely on the place of effective management or the address of the principal office to determine the residence of the Entity Crypto-Asset User.

For further details, see CARF Section IV.D(8) and Commentary thereto.

Explanation of relevant terminology - Reportable Jurisdiction

A Reportable Jurisdiction is any jurisdiction where an agreement or arrangement is in place pursuant to the automatic exchange of information under the CARF and, to facilitate the identification of Reportable Jurisdiction Persons, each jurisdiction must publish a list of Reportable Jurisdictions.

For further details, see CARF Section IV.D(9) and Commentary thereto.

Explanation of relevant terminology - Excluded Person

The term "Excluded Person" means (a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in clause (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity described in Section IV E(5)(b).

For further details, see CARF Section IV.E(1) and Commentary thereto.

80. The below sections set out the process that RCASPs should use for obtaining the valid self-certifications necessary to determine whether Individual Crypto-Asset Users, as well as Entity Crypto-Asset Users, are Reportable Users. As mentioned above. with respect to certain Entity Crypto-Asset Users, RCASPs will also need to apply an additional step to determine whether its Controlling Persons are themselves Reportable Persons who should be reported on. Each of these processes is very similar to the due diligence rules of the CRS.

Individual Crypto-Asset Users - Obtaining valid self-certifications

81. As under the CRS, a key requirement associated with the due diligence procedures for a Crypto-Asset User is obtaining a valid self-certification which establishes where the individual is resident for tax purposes. If the self-certification establishes that the Crypto-Asset User is resident for tax purposes in a Reportable Jurisdiction, then the RCASP must treat the Crypto-Asset User as a Reportable User. To this end, Participating Jurisdictions are expected to provide information to assist taxpayers to determine their residence(s) for tax purposes. In some cases, an individual may be resident in a jurisdiction for tax purposes based solely upon the individual's citizenship. If an individual is resident for tax purposes in more than one jurisdiction, all jurisdictions of residence must be included in the self-certification.

82. The self-certification can be provided in any form but in order for it to be valid the CARF sets out that it must be signed or otherwise positively affirmed, (i.e. involving some level of active input or confirmation) by the Crypto-Asset User, be dated, and must include the Crypto-Asset User's: name; residence address; jurisdiction(s) of residence for tax purposes; TIN(s) and date of birth.

Required elements for valid self-certifications for Individual Crypto-Asset Users and Controlling Persons
First and last name
Residence address
Jurisdiction(s) of residence for tax purposes
For each Reportable Person, the TIN for each Reportable Jurisdiction
Date of birth

83. Once the RCASP has obtained a completed self-certification, in order for it to be valid the RCASP must confirm its reasonableness based on the information obtained in connection with the establishment of the customer relationship, including any documentation collected pursuant to AML/KYC procedures (i.e. the reasonableness test). A RCASP is considered to have confirmed the reasonableness of a self-certification if it does not know or have reason to know that the self-certification is incorrect or unreliable.

Where a self-certification fails the reasonableness test the RCASP is expected to either obtain a valid self-certification or a reasonable explanation and documentation as appropriate supporting the reasonableness of the self-certification before it provides services effectuating Relevant Transactions on behalf of the Individual Crypto-Asset User. The Commentary to Section III of the CARF (para. 10 et seq.) contains examples of "reasonable explanation" and the applicable standards of knowledge.

Individual Crypto-Asset Users - Change of circumstances

84. A RCASP may only rely on information obtained pursuant to its due diligence procedures as long as it does not know or have reason to know that the information is incorrect or unreliable. Accordingly, if at any point there is a change of circumstances with respect to an Individual Crypto-Asset User that causes the RCASP to know, or have reason to know, that the original self-certification is incorrect or unreliable, the RCASP cannot rely on the original self-certification and must obtain a valid self-certification, or a reasonable explanation and, where appropriate, documentation supporting the validity of the original self-certification. For these purposes, a "change of circumstances" includes any change that results in the addition of information relevant to an Individual Crypto-Asset User's status or otherwise conflicts with such user's status or any change or addition of information if such change or addition of information affects the status of the Individual Crypto-Asset User.

Entity Crypto-Asset Users - Obtaining valid self-certifications

85. The due diligence procedure for Entity Crypto-Asset Users is made up of two parts:

- First, the RCASP must establish whether the Entity is a Reportable User. If so, the Crypto-Asset User is a Reportable User.
- Second, for Entity Crypto-Asset Users other than Active Entities and Excluded Persons, the RCASP must establish whether the Entity is controlled by Controlling Person(s) that are Reportable Persons(s).

Can it be determined based on information in the possession of the RCASP or that is publicly available that the Entity is not a Reportable User?

86. If a self-certification indicates that the Entity Crypto-Asset User is resident in a Reportable Jurisdiction, then the RCASP must treat the Entity Crypto-Asset User as a Reportable User unless it reasonably determines based on the self-certification or information in its possession or that is publicly available, that the Entity Crypto-Asset User is an Excluded Person. Such information includes information that was obtained for the purpose of completing the due diligence procedures pursuant to the CRS or other domestic reporting requirements (such as in relation to FATCA).

87. In determining whether an Entity Crypto-Asset User is an Excluded Person, the RCASP may follow the procedures in the order most appropriate under the circumstances. For example, as publicly traded corporations, Government Entities and Financial Institutions (other than certain types of Investment Entities) are among those Entities explicitly excluded from being Reportable Users, the RCASP may first establish on the basis of the available information described in the preceding paragraph that the Entity Crypto-Asset User is such an Entity and therefore not a Reportable User.

88. Alternatively, it may be more straightforward to first obtain a self-certification to establish that the Entity is not resident in a Reportable Jurisdiction and is therefore not a Reportable User. Participating Jurisdictions are expected to provide information to assist taxpayers to determine their residence(s) for tax purposes. In this respect, the OECD AEOI Portal contains both a compilation of tax residency rules and the information on the principles for issuance and the formats of TINs in participating jurisdictions.

Is the self-certification valid?

89. For the self-certification to be valid it must be signed (or otherwise positively affirmed, i.e. involving some level of active input or confirmation) by a person authorised to sign on behalf of the Entity, be dated, and must include the Entity Crypto-Asset User's: name; address; jurisdiction(s) of residence for tax purposes and TIN(s).

90. In addition, for the self-certification to be valid, the RCASP must confirm the reasonableness of the self-certification based on the information obtained in connection with the opening of the account (the reasonableness test). Essentially the RCASP must not know or have reason to know that the self-certification is incorrect or unreliable, based on the information obtained in connection with the establishment of the relationship, including any documentation collected pursuant to AML/KYC Procedures. If the self-certification fails the reasonableness test, a new valid self-certification would be expected to be obtained in the course of the account opening procedures.

Required elements for valid self-certifications for Entity Crypto-Asset Users
Legal name.
Address.
Jurisdiction(s) of residence for tax purposes.
With respect to each Reportable Person, the TIN with respect to each Reportable Jurisdiction.
In case of an Entity Crypto-Asset User other than an Active Entity or an Excluded Person, the information described in Section III.C(1) with respect to each Controlling Person of the Entity Crypto-Asset User, unless such Controlling Person has provided a self-certification pursuant to Section III.C(1), as well as the role(s) by virtue of which each Reportable Person is a Controlling Person of the Entity, if not already determined on the basis of AML/KYC Procedures.
If applicable, information as to the criteria it meets to be treated as an Active Entity or Excluded Person.

Controlling Persons of an Entity Crypto-Asset User -- Obtaining valid self-certifications

91. Regardless of whether an Entity Crypto-Asset User is a Reportable User, there is then a second test in relation to the Controlling Persons of Entity Crypto-Asset Users in order to identify whether they are Reportable Persons. If it is determined that the Controlling Persons are Reportable Persons, the RCASP must report information in relation to the Controlling Person as well as in relation to the Entity Crypto-Asset User that they control.

92. This second test can be broken down into two steps. First, the RCASP must ask whether the Entity Crypto-Asset User is an Active Entity or an Excluded Person. If the Entity Crypto-Asset User is neither of these, then the RCASP must identify whether the Entity Crypto-Asset User has one or more Controlling Persons which are Reportable Persons. This process is very similar to what is set out in the CRS, with the exception that the concept of "Passive NFE" (as defined in Section VIII.D(8) of the CRS) does not exist in the CARF.

Identifying whether the Entity Crypto-Asset User is an Active Entity

93. As a first step, RCASPs will need to identify whether any of their Entity Crypto-Asset Users qualify as Active Entities and should therefore be excluded from the requirements to identify their Controlling Persons. The term Active Entity essentially includes Entities with passive income consisting of less than

50% of their total income and where under 50% of their assets produce passive income (such as dividends, interest, capital gains, rents etc.). See definition of "Active Entity" in CARF Section IV.D(11) and the Commentary thereto, for further information.

Identifying whether the Entity Crypto-Asset User is an Excluded Person

94. The CARF defines Excluded Persons to mean any of the following: (a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in clause (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity described in Section IV E(5)(b) of the CARF.[16] Entities that are covered by the term "Excluded Person" are not subject to reporting under the CARF, in light of the limited tax compliance risks these Entities represent and/or the other tax reporting obligations certain of these Entities are subject to, including pursuant to the CRS. As such, the scope of Excluded Persons is, wherever appropriate, aligned to the exclusions from reporting foreseen in the CRS.

95. A RCASP may rely on the self-certification submitted by the Entity Crypto-Asset User or information that is in its possession or that is publicly available[17], including information that was obtained for the purpose of completing the due diligence procedures pursuant to the CRS, to make a reasonable determination that the Entity Crypto-Asset User is an Excluded Person. When making such a determination, the RCASP is expected to retain a notation of the type of information reviewed, and the date the information was reviewed.

Identifying Controlling Persons where necessary

96. If the Entity Crypto-Asset User is not an Active Entity or an Excluded Person, then the RCASP must "look-through" the Entity Crypto-Asset User to identify its Controlling Persons. If the Controlling Persons are Reportable Persons (i.e. are resident in a Reportable Jurisdiction), then information in relation to the Controlling Person and the Entity Crypto-Asset User they control must be reported to the jurisdiction to which the RCASP reports to so that that jurisdiction can provide that information to the Controlling Person's jurisdiction of residence. This is the same process for identifying Controlling Persons as set out under the CRS, where Controlling Persons of certain Entity Account Holders are also required to be identified.

97. To determine the Controlling Persons of the Entity Crypto-Asset User, a RCASP may rely on information collected and maintained pursuant to AML/KYC Procedures, provided that such procedures are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to Virtual Asset Service Providers).[18] If the RCASP is not legally required to apply such AML/KYC Procedures, then it must apply substantially similar procedures for the purposes of determining the Controlling Persons.

---

[16] CARF, Section IV.E(1).

[17] "Publicly available" information includes information published by an authorised government body (for example, a government or an agency thereof, or a municipality) of a jurisdiction, such as information in a list published by a tax administration; information in a publicly accessible register maintained or authorised by an authorised government body of a jurisdiction; or information disclosed on an established securities market. International Standards for Automatic Exchange of Information in Tax Matters, 2023, CARF - Commentary to Section III, para. 24: https://www.oecd-ilibrary.org/taxation/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.

[18] The Financial Action Task Force Recommendations: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Definition of "Controlling Persons"

The term Controlling Persons corresponds to the term "beneficial owner" as described in Recommendation 10 and the Interpretative Note on Recommendation 10 of the FATF Recommendations (as adopted in February 2012) and must be interpreted in a manner consistent with such Recommendations, with the aim of protecting the international financial system from misuse including with respect to tax crimes.[19]

For an Entity that is a legal person, the term "Controlling Persons" means the natural person(s) who exercises control over the Entity. "Control" over an Entity is generally exercised by the natural person(s) who ultimately has a controlling ownership interest in the Entity. A "controlling ownership interest" depends on the ownership structure of the legal person and is usually identified on the basis of a threshold applying a risk-based approach (e.g. any person(s) owning more than a certain percentage of the legal person, such as 25%). Where no natural person(s) exercises control through ownership interests, the Controlling Person(s) of the Entity will be the natural person(s) who exercises control of the Entity through other means. Where no natural person(s) is identified as exercising control of the Entity, the Controlling Person(s) of the Entity will be the natural person(s) who holds the position of senior managing official.

In the case of a trust, the term "Controlling Persons" means the settlor(s), the trustee(s), the protector(s) (if any), the beneficiary(ies) or class(es) of beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust. The settlor(s), the trustee(s), the protector(s) (if any), and the beneficiary(ies) or class(es) of beneficiaries, must always be treated as Controlling Persons of a trust, regardless of whether or not any of them exercises control over the trust. In addition, any other natural person(s) exercising ultimate effective control over the trust (including through a chain of control or ownership) must also be treated as a Controlling Person of the trust. With a view to establishing the source of funds in the account(s) held by the trust, where the settlor(s) of a trust is an Entity, RCASPs must also identify the Controlling Person(s) of the settlor(s) and report them as Controlling Person(s) of the trust. For beneficiary(ies) of trusts that are designated by characteristics or by class, RCASPs should obtain sufficient information concerning the beneficiary(ies) to satisfy the RCASP that it will be able to establish the identity of the beneficiary(ies) at the time of the pay-out or when the beneficiary(ies) intends to exercise vested rights. Therefore, that occasion will constitute a change in circumstances and will trigger the relevant procedures.

In the case of a legal arrangement other than a trust, the term "Controlling Persons" means persons in equivalent or similar positions as those that are Controlling Persons of a trust. Thus, taking into account the different forms and structures of legal arrangements, RCASPs should identify and report persons in equivalent or similar positions, as those required to be identified and reported for trusts.

In relation to legal persons that are functionally similar to trusts (e.g. foundations), RCASPs should identify Controlling Persons through similar customer due diligence procedures as those required for trusts, with a view to achieving appropriate levels of reporting.

For further details, see CARF Section IV.D(10) and Commentary thereto.

Obtaining a self-certification with respect to Controlling Persons

98. For the purposes of determining whether a Controlling Person of an Entity Crypto-Asset User is a Reportable Person, a RCASP may only rely on a self-certification from either the Entity Crypto-Asset User or the Controlling Person.

99. The self-certification can be provided in any form but in order for it to be valid the CARF sets out that it must be signed (or otherwise positively affirmed, i.e. involving some level of active input or confirmation) by the Controlling Person(s) or the Entity Crypto-Asset User, be dated, and must include the Controlling Person's: name; residence address; jurisdiction(s) of residence for tax purposes; TIN(s) and date of birth.

[19] CARF, Section IV.D(10).

100. If there is a change in circumstances that causes the RCASP to know, or have reason to know, that the self-certification or other documentation associated with an account is incorrect or unreliable, the RCASP cannot rely on the original self-certification and must re-determine their status.

Other definitions and general due diligence rules

Timing

101. A Crypto-Asset User is treated as a Reportable User beginning as of the date it is identified as such by a RCASP and the Crypto-Asset User maintains such status until the date it ceases to be a Reportable User (e.g. because the Crypto-Asset User ceases to be a Reportable User or becomes an Excluded Person, is closed, or is transferred in its entirety).

Third parties

102. Jurisdictions may allow RCASPs to use third-party service providers to fulfil their due diligence obligations. Such arrangements should include an obligation for the RCASP to make the information necessary to comply with the due diligence procedures of the CARF available to the third party(ies) fulfilling such obligations. This would include information held by the RCASP that is needed by a third party(ies) to complete the due diligence procedures. The arrangements should also ensure that the RCASP can obtain any information collected and verified in respect of Crypto-Asset Users from the third party(ies) to allow the RCASP to demonstrate compliance with the requirements of the due diligence procedures of the CARF, for instance in the framework of an audit. The RCASPs will however always remain responsible for their reporting and due diligence obligations, including their obligations on confidentiality and data protection.

103. RCASPs may also designate a single RCASP to comply with all due diligence requirements, in case multiple RCASPs provide services effectuating the same Relevant Transaction. However, the RCASP that designates the responsibilities will nevertheless remain responsible for ensuring that their due diligence obligations are fulfilled in line with the CARF.

Section 3: The information that is reported and exchanged: Reporting requirements under the CARF

104. Once Crypto-Asset Users are determined to be Reportable Users, or where Controlling Persons of Entity Crypto-Asset Users are determined to be Reportable Persons, the RCASP must report the relevant information to the tax authority. This is the information that a jurisdiction agrees to exchange with its automatic exchange partners as specified in the CARF MCAA or the equivalent.

105. The information is:

- information required for the automatic exchange partner jurisdiction to identify the Reportable Person (i.e. the Crypto-Asset User or the Controlling Person of a relevant Entity Crypto-Asset User) concerned (Identification information);
- information in relation to the relevant activity that has occurred in connection with the Reportable Person (Transaction information).

106. Together, this information should be sufficient to identify the Reportable Person and to help establish a picture of the compliance risk of that Reportable Person (i.e. whether they have properly declared the relevant transaction information concerning their Crypto-Assets or the Crypto Assets of Entities they control). The following tables set out the information to be reported in greater detail.

Identification information required to be reported in relation to Individual and Entity Crypto-Asset Users that are Reportable Users, Entity Crypto-Asset Users with Controlling Persons that are Reportable Users and the Controlling Persons themselves (same as the CRS)	
Information	*Further description (as applicable)*
Name	Name of individual or Entity concerned.
Address	The address recorded for the Crypto-Asset User or Controlling Person pursuant to the due diligence procedures. For individuals this is their current residence address.
Jurisdiction(s) of residence	This will be the jurisdiction(s) of residence identified by the RCASP pursuant to the due diligence rules of the CARF.
TIN(s)	The TIN to be reported with respect to a Crypto-Asset User or the Controlling Person is the TIN assigned to the Crypto-Asset User or Controlling Person by its jurisdiction of residence (i.e. not by a jurisdiction of source). However, the TIN is not required to be reported if either the TIN is not issued by a Reportable Jurisdiction, or if the domestic law of the relevant Reportable Jurisdiction does not require the collection of the TIN.
Information on the RCASP	The RCASP must report its name, address and identifying number (i.e. a TIN, or in the absence thereof, a business/company registration code/number, or a Global Legal Entity Identifier (LEI)), if any.

Additional identification information required to be reported in relation to Individual Crypto-Asset Users / Controlling Persons only (same as the CRS)	
Information	*Further description (as applicable)*
Date of birth	Date of birth of the Individual Crypto-Asset User or Controlling Person, as determined by the RCASP pursuant to the due diligence rules of the CARF.
Place of birth	Place of birth of the Individual Crypto-Asset User or Controlling Person, as determined by the RCASP pursuant to the due diligence rules of the CARF. The place of birth is required to be reported if, with respect to the Reportable Person, the RCASP is (i)

	otherwise required to obtain the place of birth and report it under domestic law, and (ii) the place of birth is available in the electronically searchable information maintained by the RCASP.

Information required with respect to Relevant Transactions in respect of each type of Relevant Crypto-Asset	
Information	*Further description (as applicable)*
The full name of the type of Relevant Crypto-Asset	The full name of the type of Relevant Crypto-Asset is required to be reported, and should be reported in line with the digital token identifier, where feasible.[20]
Acquisitions and disposals of Relevant Crypto-Assets against Fiat Currency	In the case of acquisitions of Relevant Crypto-Assets against Fiat Currency, RCASPs must report the aggregate amount paid net of transaction fees by the Reportable User for each type of Relevant Crypto-Assets acquired by the Reportable User. An acquisition is any transaction effectuated by the RCASP where the Reportable User obtains a Relevant Crypto-Asset, irrespective of whether such asset is obtained from a third-party seller, or from the RCASP itself. In the case of disposals of Relevant Crypto-Assets against Fiat Currency, the RCASP must report the aggregate amount received in Fiat Currency net of transaction fees for any Relevant Crypto-Assets alienated by the Reportable User. A disposal is any transaction effectuated by the RCASP where the Reportable User alienates a Relevant Crypto-Asset, irrespective of whether such asset is delivered to a third-party purchaser, or to the RCASP itself. If a RCASP only conducts one arm of an acquisition or disposal of Relevant Crypto-Assets, such that it does not have actual knowledge of the amount disposed, it is not required to report on the disposal amount and should treat the transaction as a transfer.
Acquisitions and disposals of Relevant Crypto-Assets against other Relevant Crypto-Assets	In the case of acquisitions against other Relevant Crypto-Assets, the RCASP must report the fair market value of the Relevant Crypto-Assets

[20] The Crypto-Asset Reporting Framework XML Schema and User Guide for Tax Administrationsv.

	acquired net of transaction fees. Similarly, in the case of disposals against other Relevant Crypto-Assets, the RCASP must report the fair market value of the Relevant Crypto-Assets disposed net of transaction fees.
Reportable Retail Payment Transactions	This refers to the situation where a RCASP transfers Relevant Crypto-Assets used by a customer to purchase goods or services from a merchant who receives the Relevant Crypto-Assets as consideration of goods or services for a value exceeding USD 50 000. Where a RCASP transfers payments made in Relevant Crypto-Assets from a customer to the merchant for a value greater than USD 50 000, the RCASP should report such Transfer as a Reportable Retail Payment Transaction. If the RCASP is acting as an agent of the merchant, the Transfer is reported as such and not as a Reportable Retail Payment Transaction. However, with respect to such Transfers, if the RCASP is required to verify the identity of the merchant's customer pursuant to domestic anti-money laundering rules, then the RCASP is required to also treat the customer of the merchant as the Crypto-Asset User and to report the transaction as a Reportable Retail Payment Transaction with respect to the customer. In terms of reporting requirements, aggregate information on Transfers that constitute Reportable Retail Payment Transactions with respect to a particular Crypto-Asset User is required to be reported as a separate category of Relevant Transactions. Aggregate information with respect to Transfers that do not constitute Reportable Retail Payment Transactions solely by virtue of not meeting the de minimis threshold, should be included in the aggregate information reported with respect to Transfers, and not as Reportable Retail Payment Transactions.
Other Transfers of Relevant Crypto-Assets to and by the Reportable User	RCASPs must report the fair market value of Transfers sent to, and by, a Reportable User, respectively. Where a RCASP is aware that Transfers effectuated on behalf of a Reportable User are due to certain

	types of Transfers (i.e. airdrop[21], income derived from staking, the disbursement, reimbursement or associated return on a loan, or an exchange for goods or services), it should indicate the aggregate fair market value, aggregate number of units and number of Transfers effectuated for each transfer type.
Transfers to external wallet addresses	The RCASP is required to report, by type of Relevant Crypto-Asset, the aggregate number of units, as well as the aggregate fair market value, in Fiat Currency, of Transfers it effectuates on behalf of a Reportable User to any wallet addresses (including other equivalent identifiers used to describe the destination of a Transfer) not known to be associated with a Virtual Asset Service Provider or financial institution, as defined in the FATF Recommendations.[22] Although this rule does not require the reporting of wallet addresses associated with Transfers of Relevant Crypto-Assets, to ensure that necessary information is available to tax administrations in the context of follow-up requests, a RCASP is required to collect and retain within its records, for a period not less than five years, any external wallet addresses (including other equivalent identifiers) associated with Transfers of Relevant Crypto-Assets.

General rules - transaction based reporting requirements

Reporting period

107. The information to be reported must be that as of the end of the relevant calendar year or other appropriate reporting period. In determining what is meant by "appropriate reporting period", reference must be made to the meaning that the term has at that time under each jurisdiction's reporting rules.

Valuation and currency translation rules for Relevant Transactions

108. The CARF contains a series of different currency and valuation rules that apply depending on the type of transaction that takes place. The different types of rules, according to transaction type, are described below.

---

[21] International Standards for Automatic Exchange of Information in Tax Matters - Crypto-Asset Reporting Framework and 2023 updates to the Common Reporting Standard, 8 June 2023, Commentary to Section IV.C(4): https://www.oecd.org/tax/international-standards-for-automatic-exchange-of-information-in-tax-matters-896d79d1-en.htm

[22] The Financial Action Task Force Recommendations: https://www.fatf-gafi.org/en/topics/fatf-recommendations.html

Crypto-Asset to Fiat Currency transactions

109. In general, a transaction between Relevant Crypto-Assets and Fiat Currencies must be reported in the amount of Fiat Currency paid. Where the amounts paid or received are in multiple different Fiat Currencies, the amount reported must be in a single Fiat Currency, converted at the time of each Relevant Transaction, and in a manner that is consistently applied by the RCASP.

Crypto-Asset to Crypto-Asset transactions

110. For transactions between two or more Relevant Crypto-Assets, the fair market value of the transaction must be determined and reported in a single currency. This valuation must be applied by the RCASP at the time of the transaction, in a manner consistently applied across all transactions. For example, in respect of a disposal of Relevant Crypto-Asset A against Relevant Crypto-Asset B, the RCASP could, at the time the transaction is executed: (i) perform an implicit conversion of Relevant Crypto-Asset A to Fiat Currency to determine the fair market value of the disposed Relevant Crypto-Asset A; and (ii) perform an implicit conversion of the acquired Relevant Crypto-Asset B to Fiat Currency to determine the fair market value of the acquired Relevant Crypto-Asset B. As a final step, the RCASP must sum up the total value of transactions attributable to either acquisitions, or disposals, for purposes of reporting the balance in respect of each Crypto-Asset User.

111. If there is a difficult-to-value Relevant Crypto-Asset that is exchanged for a Relevant Crypto-Asset that is more easily valued, the RCASP should rely on the valuation of the second Relevant Crypto-Asset to establish a value in Fiat Currency for the difficult to value Relevant Crypto-Asset. This valuation would then be added to the overall aggregate value for that category of transaction.

Example: A Crypto-Asset User makes use of a RCASP to dispose of Relevant Crypto-Asset A and acquire Relevant Crypto-Asset B. Relevant Crypto-Asset A has a readily obtainable Fiat Currency equivalent value and the RCASP can perform an implicit conversion to determine the fair market value of the disposal of Relevant Crypto-Asset A. However, Relevant Crypto-Asset B is a recently launched Crypto-Asset and the RCASP is not able to determine an equivalent fair market value as there is no available Fiat Currency conversion amount. In this case, to determine the acquisition value attributable to the Crypto-Asset User's acquisition of Crypto-Asset B, the RCASP can perform an implicit conversion of Relevant Crypto-Asset B by attributing to it the same Fiat Currency amount attributed to Relevant Crypto-Asset A.

Reportable Retail Payment Transactions and other Transfers

112. As for acquisitions and disposals, the fair market value of Reportable Retail Payment Transactions and other Transfers must be determined and reported in a single currency, using a reasonable valuation method that looks to the value at the time of each Relevant Transaction. The manner applied by the RCASP must be consistent across transactions. One option is for the RCASP to use as a reference the values of Relevant Crypto-Asset and Fiat Currency trading pairs it maintains to determine the fair market value of the Relevant Crypto-Asset at the time it is transferred. The information reported must also identify the Fiat Currency in which each amount is reported.

113. If the RCASP does not maintain an applicable reference value for Relevant Crypto-Asset and Fiat Currency trading pairs, then it must rely on the below valuation methods in the following order:

- firstly, the internal accounting book values the RCASP maintains with respect to the Relevant Crypto-Asset must be used;
- if a book value is not available, a value provided by third-party companies or websites that aggregate current prices of Relevant Crypto-Assets must be used, if the valuation method used by that third party is reasonably expected to provide a reliable indicator of value;

- if neither of the above is available, the most recent valuation of the Relevant Crypto-Asset by the RCASP must be used; and
- if a value can still not be attributed, a reasonable estimate may be applied as a measure of last resort.

Aggregation rules

114. Finally, for the purposes of reporting, the RCASP must aggregate (sum-up) all transactions attributable to each reporting category for each type of Relevant Crypto-Asset.

OECD
BETTER POLICIES FOR BETTER LIVES

For more information:

www.oecd.org/tax/transparency

gftaxcooperation@oecd.org

@OECDtax | #taxtransparency

OECD Tax