



KPMG AEOI Updates & Tracking Service CRS Alert



| | | | |
|-----------------------|------------------|--------------------|----------|
| Date: | 13 November 2024 | Alert Type: | Document |
| Country: | OECD | Regime: | CRS |
| Document Type: | Other Guidance | | |

OECD: Issued XML Schemas and User Guides for CARF and CRS Amendments

On 02 October 2024, the Organization for Economic Co-operation and Development (OECD) published a new crypto-asset reporting framework (CARF) XML schema and an amended version of the common reporting standard (CRS) XML schema, accompanied by user guides to facilitate the exchange of information between tax authorities under each regime.

These new XML schemas and user guides align with the CARF, and the amended CRS reporting requirements approved by OECD in 2023 and endorsed by the G20 and the Global Forum as international standards. The first exchanges under both the CARF and the amended CRS frameworks are expected to begin in 2027, for the reporting of 2026 calendar year information.

The XML schemas and user guides are mainly designed for the automatic exchange of information between tax authorities. However, jurisdictions can also mandate the use of the XML Schemas for domestic reporting by Reporting Crypto-Asset Service Providers (RCASPs) and Reporting Financial Institutions (RFIs).

CARF XML Schema User Guide

The CARF User Guide is divided into logical sections to align with the CARF XML schema, which provides comprehensive information on specific data elements and their attributes. The main sections of the User Guide are as follows:

- **Message Header:** Includes sender, recipient, message type, and reporting period.

US Contacts:



Laurie Hatten-Boyd
Principal
lhattenboyd@kpmg.com



Cyrus Daftary
Principal
cdaftary@kpmg.com

- Organization Party Type: Identifies entities such as Entity RCASPs and Entity Crypto-Asset Users.
- Person Party Type: Identifies individual RCASPs, individual Crypto-Asset Users, and natural persons controlling certain Entity Crypto-Asset Users.
- CARF Body: This section contains two sub-sections:
 - RCASP: Includes the required information about the RCASP's identity and its reporting obligation under CARF, and its nexus to the reporting jurisdiction.
 - Crypto Users: Includes information about the Reportable Users' identity and relevant transactions. These transactions include exchanges between Relevant Crypto-Assets and Fiat Currencies, exchanges between different forms of Relevant Crypto-Assets, and transfers of relevant Crypto-Assets, including Reportable Retail Payment Transactions and transfers to unhosted wallets.

Each data element and its attribute in the schema is categorized as either "Validation" or "Optional". Validation elements must be present in all data records and can be validated using automation. The sender should perform a technical check of the data file content using XML tools to ensure all validation elements are included and correct if any issues. The receiver may also check and reject the file if it is incorrect. When there is a choice between two validation elements under a validation parent and only one is required, it is indicated as "Validation (choice)."

In addition, the User Guide outlines various business rules for optional data elements in the schema:

- (Optional) Mandatory: These elements are required for CARF reporting based on the availability of information or legal factors. Notably, mandatory elements may not be present in all cases, hence a simple IT validation process may not suffice. For example, place of birth is only required if domestic law mandates it, and the information is available in an electronically searchable data maintained by the Reporting Crypto-Asset Service Provider.
- Optional: These can be provided but are not mandatory.
- Optional (non-CARF): These elements are included to maintain structural consistency with other schemas, but are not required to be reported in the CARF schema file, such as the nationality element.

Furthermore, if a sending jurisdiction identifies any inaccuracies in the information reported about the RCASP or Crypto-Asset Users, it is required to correct and submit accurate information. If the error is identified before the exchange, no correction will be

required. However, if the error is identified after the exchange, adjustments to the schema must be made per the User Guide. The CARF XML Schema includes two correctable types, RCASP and Crypto Users, to facilitate targeted reporting of corrections.

Amended CRS XML Schema User Guide

The CRS XML Schema contains updates to the existing reporting requirements that apply to CRS reporting today, adding in new data elements which are required by the updated CRS package issued alongside CARF.

The CRS Schema is largely as expected, although it is important to note that many existing fields have amended requirements applying to the content or validation of the field value.

Amongst the expected changes, there are additions to allow reporting of:

- Whether an account holder has provided a valid self-certification.
- Whether an account holder is a pre-existing or new account, by reference to the Effective date of CRS in the relevant jurisdiction.
- The type of account held – depository, custodial, cash value insurance or annuity or debt/equity interest in an investment entity.
- Whether an account is a joint account and the number of joint account holders.
- Confirmation of the requirements for reporting Controlling Person type.

Reference: [CARF XML Schema and User Guide](#), and [Amended CRS XML Schema and User Guide](#)

For information on KPMG's global AEOI network professionals, please email [GO-FM AEOI Program Support](#).

For more information on KPMG AEOI Updates & Tracking Service, please see [here](#).

For additional summaries of the latest AEOI developments, please visit KPMG's TaxNewsFlash-FATCA/IGA/CRS Insights page, [here](#).

Contact us



Cyrus Daftary
Principal
T: +1 212 954 6096
E: cdaftary@kpmg.com



Laurie Hatten-Boyd
Principal
T: +1 206 213 4001
E: lhattenboyd@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS010555-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.